"A DBS INTRUSION DETECTION AND PREVENTION SYSTEM IN WIRELESS SENSOR NETWORK"

A Dissertation Proposal
Submitted By

Amanpreet Singh

(11001612)

To
Department of Computer Science & Engineering

In partial fulfilment of the Requirement for the
Award of Degree of
Master of Technology in Information Technology

Under the guidance of

SANGEETA SHARMA
Assistant Professor, LPU

(APRIL 2015)

PAC FORM

LOVELY PROFESSIONAL UNIVERSITY

School of: SCE

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Amanpreet Singh Registration No: 11001612

Batch: 2010-15 Roll No.

Session: 2014-15. Parent Section: K2308

Details of Supervisor: Designation: AP

Name: Sanjeet Sir Qualification: MTech

UID: 15681 Research Experience: 3

SPECIALIZATION AREA: Network & Security (tick from list of provided specialization areas by DAA)

PROPOSED TOPICS

1. Distributed - Denial of Service Attack (DDOS)
2. Routing Protocal in Manet
3. QOS in Manet

Signature of Supervisor

PAC Remarks:

Chances of getting a paper published on the same are positive.

APPROVAL OF PAC CHAIRPERSON: Signature: Date: 11/10/14

**Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)

*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.

*One copy to be submitted to Supervisor.

ABSTRACT

As in the modern era the use of sensor network starts yielding a great importance in variety of applications. Thus certain research work is carried out in this particular field. The thesis will concentrates on how to conserve energy while transferring the data from sender towards receiver in a most efficient way so that the network lifetime is enhanced. Wireless sensor Networks term is refers to a kind of networking that do not requires cables to connect with devices during communication. The transmission is take place with the help of radio waves at physical level. The work would be carried out in network layer through the mechanism of routing. Networking is used to share information like data communication. A network can be wired network and wireless network. Wired network is that which used wires for communicate with each other's and wireless network is that which communicate without the use of wires through a medium. WSN Networks term is refers to a kind of networking that do not requires cables to connect with devices during communication. The transmission is take place with the help of radio waves at physical level. In the WSN sensor study the different characteristics of quality of water, temperature, density, salinity, acidity, chemical conductivity, hydrogen, dissolve methane gas and turbidity. In this work, we are going to prevent the Distributed Denial of Service, Black Hole, Sybil attacks. With this prevention we can enhance the lifetime and performance of network.

CERTIFICATE

This is to certify that **Amanpreet Singh** has completed M.Tech dissertation. Proposal titled "**A DBS INTRUSION DETECTION AND PREVENTION SYSTEM IN WIRELESS SENSOR NETWORK**" under my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

The dissertation proposal is fit for the submission and the partial fulfilment of the conditions for the award of M.Tech Computer Science & Engineering.

Date: Name: **Ms. SANGEETA SHARMA**

Signature of Advisor: UID:

ACKNOWLEDGMENT

I would like to express my sincere gratitude to my advisor **Ms. Sangeeta Sharma** for the continuous support of my thesis study, for her patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my M.Tech study.

DECLARATION

Hereby declare that the dissertation proposal entitled " **A DBS INTRUSION DETECTION AND PREVENTION SYSTEM IN WIRELESS SENSOR NETWORK"** submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date:

Investigator

AMANPREET SINGH

Reg. No. 11001612

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Wireless Sensor Network

Wireless Sensor Network are emerging as an interesting and promising area. Wireless Sensor Network be fabricated of very large number of heterogeneous/homogeneous nodes. These nodes are interconnects through wireless medium and works cooperatively to sense or monitor the surroundings. The sensor nodes in a network can vary from hundreds to thousands nodes. The nodes senses the environment and forward these information to the sink node through connected neighbours node. The sink node forward this information further to Base station. Mostly network is built only for a single application purpose. Typically WSN are used for disaster monitoring, military surveillance, Industry leakage monitoring, Health care monitoring, pollution monitoring, waste water monitoring and machine health monitoring. Since its type of applications WSN is mostly deployed in hostile environment where it is unattended. In the architecture, each sensor node consist of a radio having transceiver for communication, micro controller for processing abilities, a sensor for sensing or monitoring and battery for providing energy (Ahamed 2009).

The features of sensor nodes are

- Resource Constraint
- Unknown topology before deployment
- Unprotected and Unattended once deployed
- Unreliable wireless communication

Sensor network is infrastructure of sensing, compute and provide communication between the networking elements. Sensor network heterogeneous network self-possessed of large number of little devices known as nodes. Those nodes are forward information to Base station. A sensor network is a deployment very large numbers of little and self-organized devices that can sense, process and forward to further nodes and able to take the proper actions or decisions for that particular environment. A sensor node is detect state of a certain area like heat, motion, pressure, vibration and sound. The collected information are then forwarded to the Base station that will further processing. Wireless Sensor Network (WSN) applications are suite with IEEE 802.15.4 standards. IEEE 802.15.4 standard is for low rate Wireless Personal Area Network (WPAN) and the standard was defined for wireless

Medium Access Control layer and the Physical layer (Sohraby 2007). The characteristics of WSN are wireless medium, low cost, low power consumption and low data transmission. Further characteristics of WSN are large numbers of sensors, easily deployed, self-configurable, self-organize, collaborative signal processing and infrastructure-less. (Sohraby 2007)

Wireless sensor network is network of the small wireless modes deployed in very large scale. Wireless sensor networks sense the environment by measuring parameters as presence, temperature, pressure and humidity. Wireless sensor networks avoid the costly wired network. It is collection of small devices which provides three basic function.

- To ability to provide physical and environment conditions such as temperature, presence, moisture and pressure.
- The capability to run devices such as actuators, electric motor and switches.
- To provide effective and trustworthy communications.

WSN is a self-founding and self-healing. Self-healing networks permit nodes to reconfigure their links or paths. Self-founding permit the network itself on join of new node.

The wireless sensor network is a computer network, which is collection of large number of nodes. These nodes be situated to sensing environment around them. (Kaur 2014) These nodes are capable of fetching, sensing, storing and transferring facts. Sensor nodes can be set up anywhere without install it.

1.2 Architecture of Wireless Sensor Network

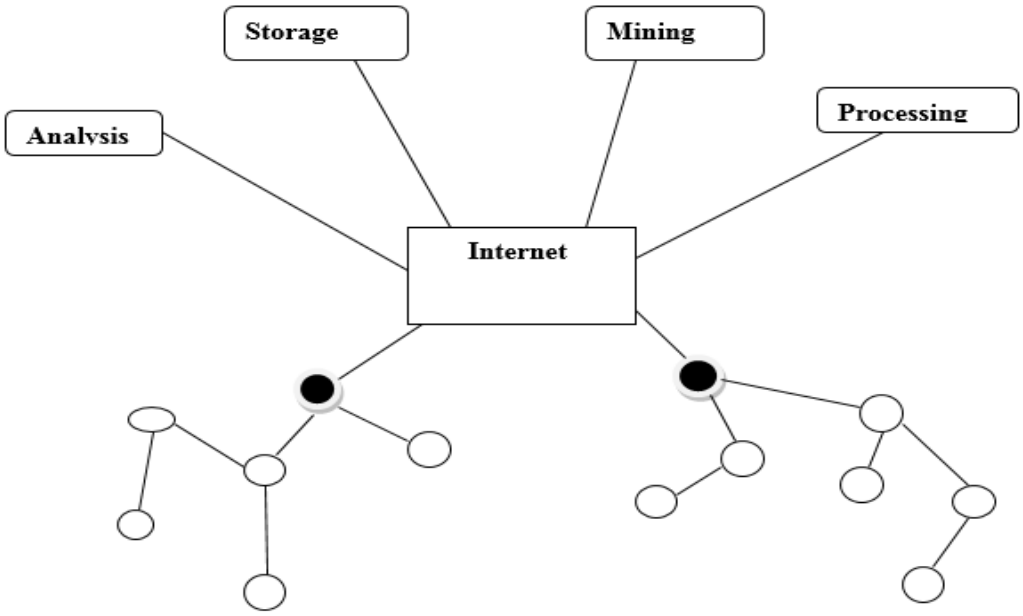

Figure 1: Wireless Sensor Network

In WSN sensors connect to the different units like Mining unit, Analysis unit, Storage unit and processing unit via Internet. The deployed network needs many large number of sensor nodes and set up in unreachable areas. The sensor node have sensing elements, with the ship processing, communication and storage abilities. The sensor node is liable for data gathering, investigation and integration of data which is gathered by that sensor node as well as the data from connected sensor nodes. Sensor nodes interconnect not only with each other but also with the Base station. In this figure it shows two sensor networks used for different regions and connecting to the Internet using their base stations. All the sensor networks the capabilities of their communication is different. For example, using infrared, ultrasound or radio frequency technologies with varying data rates and expectancies. As a final point, some nodes may have ability to extra services or technologies. For example, Global Positioning System (GPS) receivers, allowing them to accurately determine their position. However, such systems often consume too much energy to be feasible for low-cost and low-power sensor nodes. (argie 2010)

1.3 What is Sensor and its Architecture

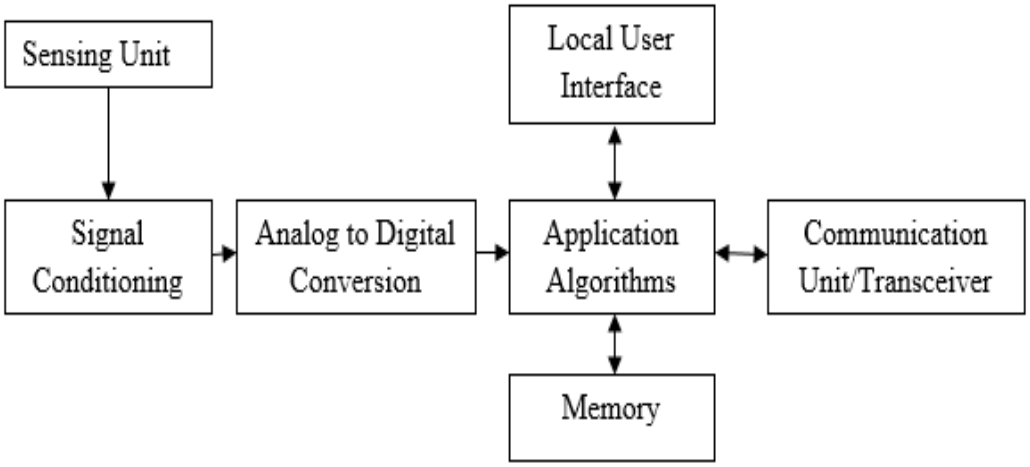

Figure 2: Basic Architecture of Sensor

A sensor node is a mixture of sensing, processing and communication techniques. The sensing unit senses the change of constraints, signal conditioning circuitry prepares the analogy signals to convert into the digital signals, the sensed data is converted and is used as the input to the processing unit, the memory helps processing of tasks and the transceiver is used for communicating with the base stations or sink node .Sensors can monitor temperature, vehicular movement, object movement, pressure, humidity, noise levels, lighting conditions, the presence or absence of certain kinds of substances, mechanical stress levels on objects and some other properties. Their mechanism may be thermal, visual, magnetic, seismic, infrared, acoustic or radar. A sensor is able of self-identification and self-diagnosis. The mechanisms of sensors work in three ways: by a line of sight to the target as visual sensors, by proximity to target as seismic sensors and by propagation like a wave with possible bending.

1.4 MAC (Medium Access Control)

The main functioning on the data link layer before the transmission is medium access control known as MAC. It used to provide good network throughput, network performance, energy consumption and delivery of the data. However, MAC protocols for wireless networks cannot be applied directly to any sensor networks without adjustment because it never take into interpretation the unique characteristics of sensor networks, in particular the energy limit. For example, in the cellular system the main thing is to be responsible for

quality of service to users. Energy efficiency is only of minor significance because there is no power limit with the base stations and the mobile users can replace the batteries in their handsets. In MANETs, nodes are furnished with portable devices powered by battery, which can be replaceable. So a very big quantity of research work has been accompanied on Media Access Control. (Ali 2006)

1.5 Characteristics of MAC protocol

- **Energy Efficiency:** Sensor nodes must operate using finite energy sources (batteries), therefore MAC protocols must be energy-efficient. Since MAC protocols have full control over the wireless radio, their design can contribute significantly to the overall energy requirements of a sensor node. A common technique to preserve energy is described as dynamic power management (DPM), where a resource can be moved between different operational modes such as active, idle, and asleep. For resources such as the system, the active mode can group together multiple different mode of activity, for example, transmitting and receiving. Without power management, most transceivers switch between transmit, receive, and idle modes, although they receive and idle modes are typically similar in their power consumption. However, dramatic energy savings can be obtained by putting the device into the low-power sleep mode. (argie 2010)
- **Reliability:** It is a common requirement for most communication networks. The design of the MAC protocol can increased reliability by identifying and improving from communication errors and collisions using acknowledgments and retransmissions. In wireless sensor networks, where node failures and channel errors are common, reliability is a main concern for many link-layer protocols.
- **Throughput:** The Throughput is term which describe the amount of data is successfully delivered to one node to another node or source to the destination in bits or bytes per second. It is affected by many factors. The effectiveness of channel utilization, overhead, collision avoidance and potential. As potential, the significance of throughput depends on different applications.
- **Low Latency and Predictability:** Many WSN applications have timeliness requirements, that is, sensor data must be collected, combined, and delivered within certain latency constraints or deadlines. For example, in a network that monitors the spreading of a wildfire, (Shiri 2012) sensor data must be delivered to monitoring

stations in a timely fashion to ensure accurate information and timely responses. Numerous network activities, protocols, and mechanisms contribute to the delays experienced by such data, including the MAC protocol. For example, a large frame size and a small number of slots allocated to a node in a TDMA-based protocol lead to potential delays before critical data can be transmitted over the wireless medium. In a contention based protocol, nodes may be able to access the wireless medium sooner, but collisions and the resulting retransmissions incur delays. The choice of MAC protocol can also affect how predictable the experienced delay is (Sohraby 2007), for example, expressed as upper latency bounds.

- **Scalability:** In the wireless medium access control protocols have been deliberate for use in substructure-based systems, where every nodes can access to the channel and achieve some central management and controlling functions. Most wireless sensor networks depend on multi-hop and peer-to-peer communications without centralized synchronization. MAC protocols must be able to allow for efficient use of resources without incurring improper overheads, in very large networks. For example, centralized protocols would incur significant overheads for the distribution of medium access schedules and are therefore unsuitable for many WSNs. MAC protocols based on CDMA may have to cache a large number of codes, which may be impractical for resource-constrained sensor devices. In general, wireless sensor nodes constrained in their energy resources, handling and memory capacities. Therefore, protocols must not carry out excessive computational burden.
- **Channel Utilization:** The Channel Utilization is term in which bandwidth consumption for actual communication. But cause of limited bandwidth, the protocols must make use of the bandwidth as resourcefully as thinkable.
- **Adaptability:** Wireless Sensor Network is its capability to self-manage, it can adjust to modifications in the network, like modifications in topology, network size, density and traffic appearances. The protocols for a Wireless Sensor Network must be able to familiarize modifications starved of extra control overheads. The protocols that make medium access choices based on current network state and there routing paths. Protocols with fixed preps may suffer from large overheads lack of variations of those preps that can affect all nodes or whole network. (Ali 2006)

1.6 Challenges for the WSN

- **Energy:** The major factor in sensor network design is that sensor nodes function with limited energy costs. Sensors are powered with the help of batteries, which must be either replaced when useless, recharge battery using solar power. They will throw away once their energy source is depleted. Whereas non-rechargeable batteries, a sensor node should be able to operate until the battery can be swapped. The most important design challenge is energy effectiveness. This constraint imparts all side of sensor node and its network design.
- **Self-Management:** This is the primary behaviour of any Wireless Sensor Network that they must operate in remote regions and unattended situations, without the probability for maintenance and patch-up. (Shiri 2012) So sensor nodes must be self-managing in that they organise themselves, function and cooperate with other nodes, changes in the situation.
- **Decentralized Management:** Central management of the network often not possible due to large scale of networks and power restrictions. So decentralized systems favoured, though they may perform poorer than their centralized complements. Each sensor makes routing decisions based on boundless local information. Paths may be non-optimal, but path establishment management can be much cheaper.
- **Design Restrictions:** the hardware and software boundaries affect the whole system design, like low cost, less energy consumption, long life and reduce software complexity.
- **Security:** All sensor networks gather sensitive information. The sensor network are mostly so far and critical environment so the numbers of attacks and malicious intrusions are increases. The wireless system is easy to take the eavesdrop of whole network on each transmission. In these days the Distributed denial-of-service attacks are more popular to interpret the working of our wireless system. This can happen using a large variety of attacks like jamming attack, in which the attack forward large number of packets to shut down the network for legitimate nodes. There is not universal solution to detect and prevent these type of attacks. The detection and prevention of these attacks depends upon the Applications or Networks. (Walters 2007)

1.7 Applications of WSN

- **Military Applications:** The Wireless Sensor Network is the most used system in military command, control and communication. WSN can deployed in the battlefield in critical situations without any pre-existing network and used to take the next action or decisions according to the information sensed by the our deployed network. So we do not need to taking care of that areas where the human involvement is too difficult. In the battlefield we can sense the presence of the enemy, any vehicles or other objects. We also can activate our weapons when enemy or other activity sensed at that places.
- **Industrial Applications:** In this areas we can used the wireless sensor networks to collect the information about any industrial place. We can monitor the situation like leakage, fire or any other unwanted condition. For example, if leakage is started in some part of the gas line, the sensor network will activate and forward the information of that particular area to the Base station.
- **Environment Monitoring:** It is very earliest applications of the WSN. These applications monitor the environment using some parameters. The popular applications in this field are Air or Water quality monitoring, Disaster monitoring, Plant growth in the forest areas, Fire detection in forest etc.

1.8 Models Use in WSN

Components of Sensor Node: A sensor node is made by the four basic components. Such as,

- Sensing unit
- Processing unit
- Transceiver unit
- Power unit

The sensor node also has some additional features. Such as,

- Location finding system
- Power generator
- Mobilize

The sensor node has the two sub units. Such as,

- Sensors
- Analog to digital converter

In the WSN Analog to digital converter is used. The sensor nodes are produced the analog signals hence these signals are converted to digital signals by the use of ADC. After that the digital signal is result in the form of processing unit. The processing unit is use to assign the sensing tasks to the various nodes. The processing unit is generally the small storage unit. It is used to manage the various tasks that are helpful in producing the sensor nodes. The transceiver unit is helpful in connect the nodes to the network. The other component of the sensor node is power unit. The power unit is helpful in saving the power consumption in the network.

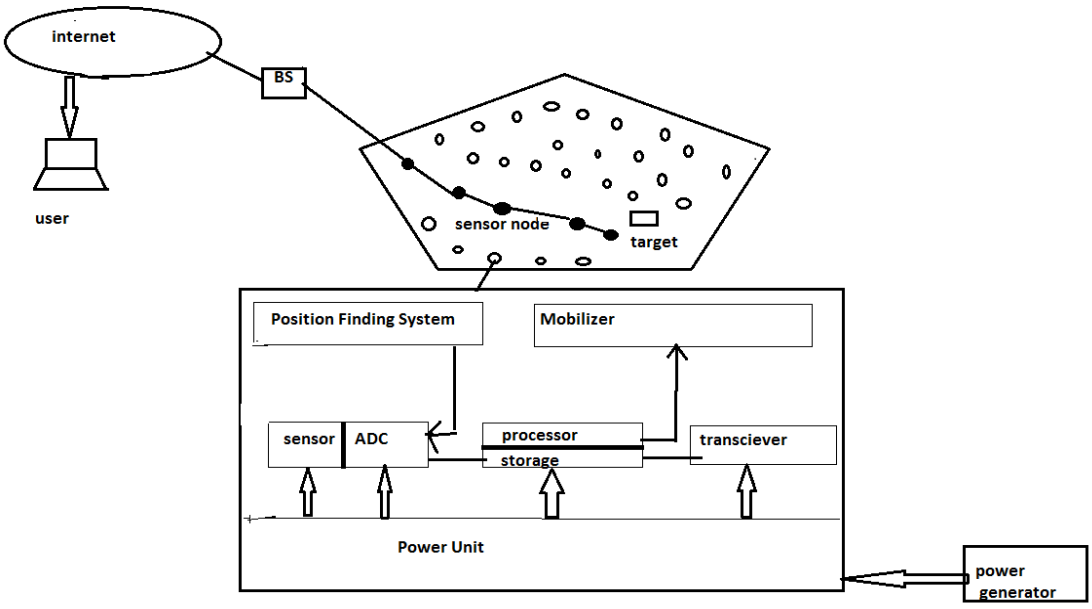

Figure 3: Component of Sensor Nodes

In the WSN network the microprocessor is used. The microprocessor has the many functions as,

- Managing data collection from the sensors
- Performing power management functions
- Interfacing the sensor data to the physical radio layer

- Managing the radio network protocol

The wireless sensor nodes are used to minimize the power consumption of the system. The radio subsystem requires the large amount of power to communicate in the network. That's why we sent the data over the radio network when it is required.

1.9 Advantages of WSN

- The WSN is flexible and it goes through the any physical partitioning
- The WSN accommodate the new devices at any time
- WSN is used to avoid the lots of wiring
- WSN can be accessed through the centralized monitors
- It has the advantage of robustness
- It provides the feature of scalability i.e. can be expanding from smaller network to larger network
- It avoids the use of lots of wiring
- It can add device at any time
- Through centralized monitor it can be accessed
- It is flexible in nature

1.10 Disadvantages of WSN

- The WSN are very costly
- WSN are easily get distracted by the various devices such as Bluetooth
- It is easy for the hackers to hack a WSN. Because the control of the propagation waves is not possible
- The communication speed is relatively low then the other networks
- It can be hack easily as we cannot control propagation of waves. So it is not secure network.
- It has low speed of communication as compared to wired network
- It is highly expensive network
- It is highly complex system
- It gets easily distracted with the interference of other devices like Bluetooth

1.11 Characteristics of WSN

The main characteristics of WSN are:

- It provides mobility of nodes
- WSN has ability to cope with failure of nodes
- Power consumption constrains for nodes using batteries or energy harvesting
- Communication failures
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use

Each square cell may have four dissemination nodes at its four corners. A request from the sink may include one of these four dissemination nodes in its path to the sink. The Multiple sink could be present at any place in the sensor field and thus request can be generated from anywhere in the sensor network. The sensor networks has the capability of sensing, computing and gathering information.

1.12 The Sensor Node Architecture

Sensor nodes are driven by battery and have very low energy resources which effects the network lifetime. Block diagram of sensor node is shown in below figure.

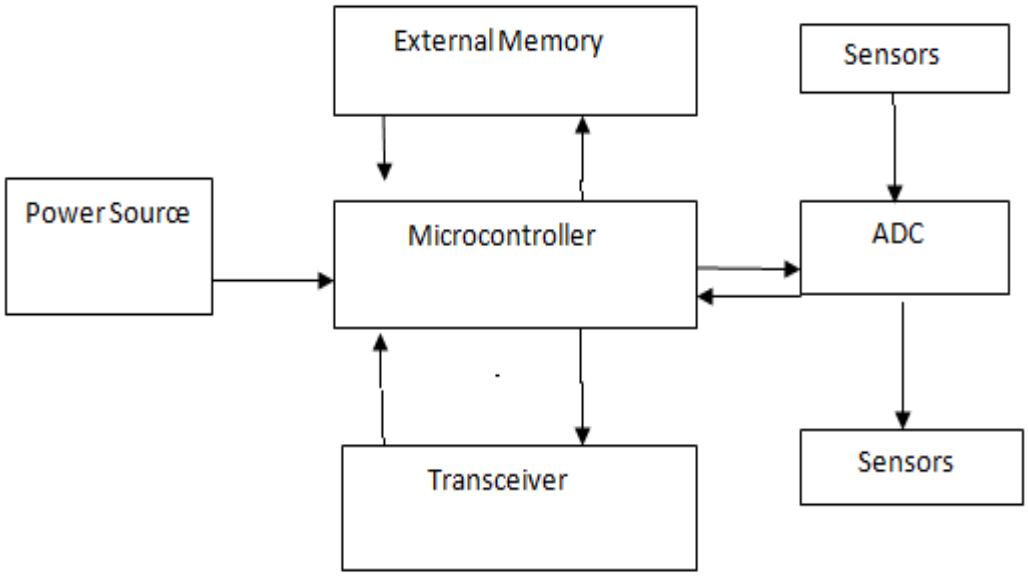

Figure 4: Block diagram of sensor node

1.12.1 Components of a Sensor Node

Sensor node consists of following major components:

- **Microcontroller:**

  It is suited for sensor nodes due to their flexibility to connect to other devices. It performs tasks after that process information and then controls the functionality of other components.

- **Transceivers:**

  The transceiver provides the functionality of both transmitter and receiver. Radio Frequency communication is best suited for sensor networks. Sensor network use the frequency between the range of 433Mega hertz and 2.4 gigahertz.

- **External memory:**

  Two kinds of memory are used on the basis of type of storage: user memory for Storing application related or personal data and programming memory for program the device.

- **Power Source:**

  Batteries are the main source for sensor networks. Sensors can sense, store and gather information. For all this they consume power.

- **Sensors:**

  Sensors are the small tiny partials which sense, store and gather information. Sensor node consists of three components: sensing, processing and communicating. Sensor is a device that responds to a change in its surrounding in a measurable manner. There are two types of sensors active and passive. Active sensor gathers data by probing into the environment, while passive sensors gather data without actually disturbing the environment.

- **ADC:**

  ADC is an analog to digital convertor that allows exploiting the information-theoretic redundancy of the input signal for increasing the efficiency of operation and reducing the power consumption of the converter.

1.13 Applications of WSN

Wireless sensor network has many applications in various fields.

- **Military Applications**

  Wireless sensor networks can be used in the application of control, communications, computing, intelligence, surveillance, military command, reconnaissance and targeting systems. In the battlefield context, rapid deployment, self-organization, fault tolerance security of the network should be required. The sensor devices or nodes should provide following services:

  - Monitoring friendly forces, equipment and ammunition
  - Battlefield surveillance
  - Reconnaissance of opposing forces
  - Targeting
  - Battle damage assessment

- **Environmental Applications**

  Now sensor networks are also applied in traffic control, habitat monitoring and agriculture etc. because there is no interruption to the environment. Bush Fire Response: A low cost distributed sensor network for disaster response and environmental monitor. An integrated network of sensors combining on the ground sensors monitoring humidity, wind speed, local moisture levels, and direction, together with satellite imagery and longer term meteorological forecasting will enable the determination of fire risk levels in targeted regions as well as valuable information on probable fire direction. Such a network will provide valuable understanding of bushfire development and most importantly assist authorities in organizing a coordinated disaster response that will save lives and property by providing early warning for high risk areas.

- **Patient monitoring**

  Sensor networks are also widely used in health care area. In some modern hospital sensor networks are constructed to monitor patient physiological data, to control the drug administration track and monitor patients and doctors and inside a hospital. In spring 2004 some hospital in Taiwan even use RFID basic of above named applications to get the situation at first hand. Long-term nursing home: this

application is focus on nursing of old people. In the town orientation sensors, farm Cameras, pressure sensors, and sensors for detection of muscle activity construct a complex network. They support fall detection, unconsciousness detection, vital Sign monitoring and dietary/exercise monitoring. These applications reduce personnel cost and rapid the reaction of emergence situation.

- **Home appliances**

  Along with developing commercial application of sensor network it is no so hard to image that Home application will step into our normal life in the future. Many concepts are already designed by researcher and architects, like "Smart Environment: Residential Laboratory" and "Smart Kindergarten". In the concept "the intelligent home", when you come back home. At the front door the sensor detects, you are opening the door and then it will tell the electric kettle to boil some water and the air condition to be turned on. You sit in the sofa lazily. The light on the table and is automatically on because the pressure sensor under the cushion has detected your weight. The TV is also on. One sensor has monitored that you are sitting in front of it. "I'm simply roasting. The summer time in Asia is really painful." You think and turn down the temperature of the air condition. At the sometime five sensors in every corner in the room are measuring the temperature. Originally there is also sensor in the air condition. But it can only get the temperature at the edge of the machine not the real temperature in the room. So the sensors in the room will be detecting the environment. The air condition will turn to sleep mode until all the sensors get the right temperature. The light on the corridor, in the washing groom and balcony are all installed with sensor and they can be turned on or turn out automatically.

- **Security monitoring**

  Security monitoring networks are collection of nodes that are placed at fixed locations throughout an environment that continually monitor one or more sensors to detect an anomaly. In a collection tree, each node must transmit the data of all of its decedents. The accepted norm for security systems today is that each sensor should be checked approximately once per hour.

1.14 Design Issues and Challenges of a Wireless Sensor Network

- Random deployment -autonomous setup & maintenance
- Infrastructure-less networks -distributed routing
- Energy, the major constraint -trading off network lifetime for fault tolerance
- Accuracy of results
- Hardware energy efficiency
- Distributed synchronization
- Adapting to changes in connectivity
- Real-time communication, quality of services.

1.15 Energy Consumption Issues in WSN

Energy consumption is one of the main issues in wireless sensor networks. It is the important factor which determine the lifetime of a sensor network which is driven by battery. Sometimes the energy optimization become complicated in wireless sensor networks because it is not only involved the issue of energy consumption, but the prolonging of battery life as much as possible. The optimization of energy can be done with the awareness of energy as design aspects. Different types of algorithms and protocols were developed to minimize the energy consumption of the network sensor. The lifetime of a sensor network can be increased by making the operating system, the application layer and the network protocols are designed to be energy aware. These protocols and algorithms have the special features of microprocessor and transceivers to minimize the sensor node energy consumption. Different types of designs are developed for energy consumption awareness.

1.16 Routing Protocols

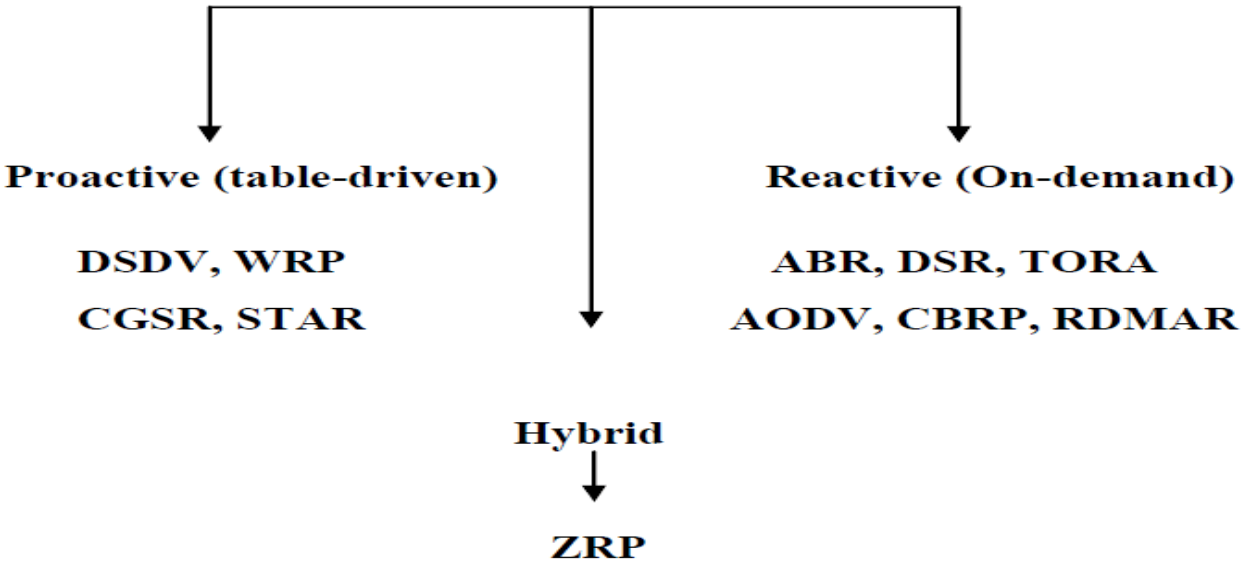

Figure 5: Ad-hoc routing protocols

In ad-hoc networks to ensure the delivery of packets from sender to destination each node must run a routing protocol and maintain routing table in the memory. Routing table can be classified into two categories: reactive and proactive and hybrid.

1.16.1 Reactive Protocols

In the reactive protocols also called an on demand routing protocol topology data is given only when needed. In the network when node wants to know the route to destination node it floods the network with a route request message. It gives a reduced average control traffic, with bursts of messages when packets need being routed and an additional delay due to the fact that the route is not immediately available.

- **DSR (Dynamic source routing)**

  Dynamic source routing is a on demand protocol. It is based on the concept of source routing. The mobile nodes are used to maintain the route memory. It is used to contain the source route. In the route cache the entries are continuously updated. The protocol consists of two major phases: route discovery, route maintenance. When mobile nodes send to some destination, it first consults its route cache to determine whether it already has a route to the destination, it will use this route to

send packet. This route request message contains the address of destination, along with the source node address and unique identification number.

- **AODV (Ad hoc on-demand distance vector routing)**

  It is distance vector protocol. In this process source nodes send message to some destinations it initiates a path discovery process to locate the other node. It is used to broadcast route request packet to its neighbour nodes. Then it forwards the request to their neighbours. AODV uses destination sequence numbers to ensure all routes are loop free contain the most recent route information. Each node maintains its own sequence number as well as broadcast ID. Afterward RREP message is unicast by the destination to the originator of the RREQ.RERR, and other message of RERR (route error) message are used to notify nodes about link breaks.

- **DSDV (Destination-sequence distance-vector routing)**

  This routing is a table-driven routing protocol. Which requires each node to advertise its routing able to its neighbours? Route information contains a route sequence number, the destination distance in hops, and the sequence number of information received regarding the destination as stamped by the destination itself.

1.16.2 Proactive protocols

In the case of proactive protocols are characterized by periodic exchange of topology control messages. Nodes periodically update their routing tables and control traffic is more dense but constant and routes are instantly available.

- **OLSR (optimized Link State Routing)**

  The optimized link state routing protocol is proactive link state routing protocol for ad hoc network. OLSR is a flooding mechanism, it is used for distributing link state information. It broadcast the information to all other nodes. OLSR used in the particular for large and dense networks. It used to control the traffic between various nodes. It helps to exchange the two type of messages, these messages are hello messages and topology control message. Hello messages are exchanged periodically among neighbour nodes in order to detect links to neighbours. Topology control messages periodically flooded to entire network in order to

diffuse link state information to all nodes. In the OLSR protocol used the multiple interface declaration and host and network association to avoid collisions.

- **OSPF (open shortest path first)**

  It is a link state routing protocol and issued from the very first link state protocol. It is used in Arpanet packet switching network. In this routing OSPF maintain information of the network topology in the database stored in every node. In the database build a shortest path tree to route a packet to its destination. Neighbour discovery of any node can be accomplished through exchange of hello packets.

- **FSR (fisheye state routing)**

  FSR is a scalability-supporting link state protocol. In this routing every node broadcast links to state information to its destination neighbours and their frequency inversely proportional to destination distance in hops. Every node has precise knowledge of its local neighbours with the knowledge of distant nodes is less precise. This makes the routing of a packet accurate near the source and destination. In this of FSR is used in large networks.

- **ADV (adaptive distance vector routing)**

  In the ADV protocol also has some reactive characteristics. In this protocol every node shares its route information with its neighbours according to bellman ford distance vector algorithm. ADV node maintain route to nodes that are recently active connection.

- **STAR (Source tree adaptive routing)**

  In this routing protocol use the source tree and computed by every node in order to route packets. Every node then shares its whole tree with the help of its neighbours.

- **WRP (wireless routing protocol)**

  This protocol based on the path finding algorithm. In the WRP each node shares its routing information or tables with the neighbours with the help of communicating the distance and second to last hop to each destination.

1.16.3 Hybrid Protocols

Hybrid protocols has the both properties of reactive and proactive in nature. Network divide into different regions like inside it's near neighbourhood regions and outside this region. There are two types ZRP (zone routing protocol) and CBRP (cluster based routing protocol).

- **ZRP (zone based routing protocol)**

  All the nodes in this protocol define in the radius it is inside which packets are routed using proactive routing protocol. All the rotes those are outside the radius it is discovered by the reactive protocol. In this protocol itself three protocols like IARP (intra zone routing protocol) IERP (the reactive inter zone routing protocol) BRP (broader cast resolution protocol).

- **CBRP (cluster based routing protocol)**

  It divides the network into overlapping or disjoint node clusters. Every cluster has 2 hopes in the diameter. Every cluster has one head and its duty has to exchange route discovery messages with other cluster heads. Proactive routing protocol is used inside every cluster further inter-cluster routes are discovered via route requests.

CHAPTER 2

REVIEW OF LITERATURE

Intanagonwiwat et al (2000)," A Scalable and Robust Communication Paradigm for Sensor Networks" proposed **Direct Diffusion** which is a data centric protocol, in which main idea is based on diffusing data through sensor nodes using naming scheme for data based on interest in communication. A query broadcasted by the sink through its neighbors .And interested nodes can send data in response to the query. The interest entry also contains several gradient fields. A gradient is a reply link to a neighbor from which the interest was received. It is characterized by the data rate, duration and expiration time derived from the received interest's fields. Hence, by utilizing interest and gradients, paths are established between sink and sources. Several paths can be established so that one of them is selected by reinforcement. Thus it will result in using the efficient path which will consume less power. If the path fails between source and sink then an alternative path is utilized. Thus it will increase the overhead by keeping the alternatives paths. Thus it may not be possible to be applied to large sensor networks.

Ian F., Akyildiz *et.al* (2002), "Wireless sensor networks: a survey" have presented electro-mechanical systems technology. Sensing tasks and potential sensor networks are also explored and also define the factor influencing the design of sensor networking. High sensing, fault tolerance, flexibility and low cost characteristics make different types of application. They also explained about pre-defined and development phase and re-deployment of additional phases. (Akyildiz 2002)

Lindsey et al (2002)," Power Efficient Gathering in Sensor Information Systems (PEGASIS)" it is an enhanced version of LEACH protocol. That is a chain based protocol provides improvement over LEACH algorithms. Each node aggregates the collected data with its own data and then passes the aggregated data to the next node in the chain and finally to the designate node which transmits it to BS. Using greedy algorithm, the nodes will be organized to form a chain, after that BS can compute this chain and broadcast it to all the sensor nodes. Energy saving in PEGASIS over LEACH takes place by many stages: First, in the local data gathering, the distances that most of the sensor nodes transmit are much less compared to transmitting to a cluster-head in LEACH. Second, only one node

transmits to the BS in each round of communication. Also the number of transmissions to BS is reduced. It employs multi hop transmission and selecting only one node to transmit the data to the sink or base station while in LEACH it uses single hop. Since the overhead caused by dynamic cluster formation is eliminated.

For larger networks, PEGASIS adds excessive delay for distant nodes. And the single designated node can be a bottleneck which is responsible to transmit the data to BS. It is based on some assumptions which make solutions not practical in real world like any node can send information directly to base station. And all nodes are aware of locations of sensor nodes in WSN.

Karlof, Chris and David Wagner (2003), "Secure routing in wireless sensor networks: Attacks and countermeasures" In this paper, the technology advances in Micro-Electro-Mechanical Systems which has assisted the development of sensors, we have seen that in very few last years the development and deployment of WSNs in military, environment, surveillance, natural disaster relief, healthcare. These WSNs carry the promise of drastically improving and expanding the quality of services across a wide variety of settings and for different segments of the population. The sensor node provide authentication using Zero Knowledge Proof (ZKP) to add new node in the network then add that node in the cluster. The cluster head selected on the basis on the strong parameters like connect up time, bandwidth performance and battery lift of all the neighbouring nodes. (Karlof 2003)

Diamond et.al (2007),” Application of wireless sensor network to military information integration” has presented different types of applications in the field of WSN. WSN is used in military applications, health applications, home appliances, environment applications. All these applications have the different impact on each field. The features of these applications are depends on how and where we use or implement wireless sensor network. According to the applications the sensed information and processing on it changes. (Diamond 2007)

Tarique Haider and Mariam Yusuf (2009),” A Fuzzy Approach to Energy Optimized Routing for Wireless Sensor Networks” discussed about the approach that is based upon the fuzzy logic. This approach is used as the energy awareness approach. It is soft, hence it can accommodate sensor networks comprising of different types of sensor nodes having different energy metrics. In this paper, they present a fuzzy model for energy aware routing in wireless sensor networks. Existing proposed routing protocols for WSNs use fixed

metrics for making energy aware routing decisions. This has the disadvantage of not being easily adaptive to changes in sensor types because energy metrics vary widely with the type of sensor node implementation platform. Some of the factors for calculating routing metric are conflicting. For example, short multiple hops reduces transmission power but results in greater number of hops thereby reducing the energy of a larger number of nodes involved in relaying. Fuzzy logic, on the other hand, has potential for dealing with conflicting situations and imprecision in data using heuristic human reasoning without needing complex mathematical modelling. The potential of fuzzy logic is being fully explored in the fields of signal processing, speech recognition, aerospace, robotics, embedded controllers, networking, business and marketing. In this work, they present a soft, tune able parameter based approach to energy optimized routing using fuzzy variables and rule base. This results in soft accommodating way of routing in WSNs capable of handling a wide range of energy metrics of different sensor implementation platform. They assumed a cluster-based architecture for WSN, where a group of nodes is managed by a gateway. Various criteria for cluster-formulation have been proposed but in this paper focus is on routing within a cluster. The gateway is responsible for the management of nodes in its cluster, communicating with other gateways, processing of data received from sensor nodes and transmitting the processed data to the command centre. They considered that the gateway is much powerful as compared to sensor nodes and has no energy limitations. All sensor nodes have one destination namely the gateway. They presented a novel fuzzy model for energy optimized routing in wireless sensor networks. Simulation results have demonstrated the reliability and efficiency of this approach. Moreover, as fuzzy approach is soft it can be easily tuned for different network and node conditions simply by changing shapes of the fuzzy sets.

Selcuk Okdem et.al (2009)," Routing in WSNs Using an Ant Colony Optimization (ACO) Router Chip" has explained about the stable nodes. Ant colony optimization is based on swarm intelligence. A novel Routing technique using Ant colony optimization algorithm is proposed in the WSNs. Comparative and descriptive study is also mentioned in this paper. It is also implemented on small size component. Adaptive method is established with the help to the objective, their main aim was to maintain maximum life time and so that data receive become efficient. The proposed ACO approach for routing and its implementations is the solutions for node designer. (Okdem 2009)

Pathania, Shruti et.al (2010), "Energy Efficient Mechanism to Enhance the Life Time of Wireless Sensor Network" have discussed about metrological approach with different types of magnitudes of parameters like temperature, humidity and discussed all the conditions to trace the weather conditions. A radiation shield is also developed to study the influence of climate and develop a temperature correction model. Classes of data will be defined on the basis of instruments calibration procedures, method, frequency, traceability chain etc. (Pathania n.d.)

Cheick Tidjane Kone, Michael David, and Francis Lepage, (2010)," Multi-channel Clustering Algorithm for improving Performance of Large-Scale Wireless Multi-Sink Sensor Networks" has discussed the distributed clustering algorithm. It is suitable for large scale wireless sensor networks. It consists of sensor nodes and sink nodes. A two tiered hierarchical architecture is used to increase scalability and ensure performances and durability of system. A multi-channel system is used to create a cellular structure by assigning one frequency channel per cluster. The simulation technique is used to evaluate and compare the impact of two distributed schemes. The connectivity and the scalability of the network are important design goals to ensure network performance. The hierarchical architectures are used to solve the scalability problem. In the WSN, the network is partitioned into several groups. For optimizing the energy and communication efficiency in the clusters, the multi-channel system can be used. For this, cellular network approach is used to assign the frequency channel per cluster. In this paper author propose simple and distributed clustering algorithm which use multiple sinks and frequency channels to improve the performance.

Xu, Li et.al (2010)," Sink Mobility in Wireless Sensor Networks" In this proposed paper we know about the collected data from the nodes for analysing and uses of it. They explained the balancing of the load battery depletions and movement of the sink node. They deliberated the computation power of sink node and performance of the whole Wireless Sensor Network. They deliberated about the most coming problems in WSN and sing node and give the overview of the models and assumptions. (Li 2010)

Chaurasiya, et.al (2011)," An Enhanced Energy-Efficient Protocol with Static Clustering for WSN, Information Networking" proposed a new routing technique. As Wireless Sensor Networks consists of a large number of sensor nodes. These sensor nodes are connected through wireless medium. In the WSN the energy efficiency is the basic need. In this case, author propose an energy-efficient routing scheme called Enhanced Energy-Efficient

Protocol with Static Clustering (E3PSC) which is basically a modification of an existing routing scheme, Energy-Efficient Protocol with Static Clustering (EEPSC). The qualitative and quantitative analysis is performed to establish the claim of energy efficiency of the proposed scheme. As, Enhanced Energy-Efficient Routing Protocol in wireless sensor network is a demanding task. This demand has led to many routing protocols. Most of these protocols find the minimum energy path or the shortest path routing. Always using these paths will soon make those nodes to lose their lifetime. Based on our experimental results, it has been found that E3PSC outperforms EEPSC in terms of network lifetime and energy consumption.

Mario Collotta et.al (2011)," A fuzzy based algorithm to Manage Power Consumption in Industrial Wireless Sensor Networks" has discuss about the use of WSN in industry. As now days, network plays an important role in WSN. It used to control the sleep and the wake times of the nodes. It helps to make data transmissions in an energy efficient way. The main aim of the wireless industrial network is to meet the requirements of industrial applications. The industrial communications of the network guarantee high reliability, low power consumption. There are huge factories, which may include the large number of nodes and high node density. The main role of industrial WSN is to creating a highly reliable and self-healing industrial system. This system helps to responds in real time events with appropriate actions. The nodes activities have to last for a long period of autonomy, in order to prolong the lifetime of the nodes and the lifespan of the network. In this paper, a new energy management approach is purposed. It is able to increase significantly the overall network lifetime through a sleep/wakeup policy based on fuzzy logic algorithm. Our goal is to create a time driven approach that awakens the nodes only when they are really meant to convey. The aim of this paper is to show how, using a fuzzy logic controller, implemented in an industrial WSN, it is possible increasing the life cycle of the batteries of the individual wireless nodes and by exerting continuous control on energy consumption of individual nodes.

Naveen et.al (2011),"Cooperative Data Caching in WSN" In this paper the cooperative caching structure ZCS to increase the performance of WSNs. The structure is used to share their data for zone nodes in which it displays limited nodes problems and limited query potential at a node to extend period of WSNs. A cache discovery process, distance based admission control, consistency check and utility based cache replacement policy is include

by ZCS scheme. For the increment in the hit ratio replacement policy is used. (Chauhan 2011)

Kiran Maraiya et.al (2011),"Application based Study on Wireless Sensor Network" This paper defined indication of WSN (wireless sensor network).Then it shows that how it changed from other networks like Ad-hoc or MANET. They about the existing problems, design challenges and concern the advantages of the protocols used Wireless Sensor Network. They deliberate the main network topologies used in the network, what are the different types of its applications, constrain and protocol stack architecture. (Kant 2011)

Sanaei, Zohreh et.al (2012) "SAMI: Service-based arbitrated multi-tier infrastructure for mobile cloud computing" This paper proposes the use of virtualization for application offloading with the mobile Computing. In mobile cloud computing, application offloading is implemented as a software level solution for augmenting computing potentials of smart mobile devices. In cloud environment we come across different software's which can be used to access information or for information management, but to do so, we cannot use mobile devices because their architecture and design are not compatible with that of the software's. Therefore, the application offloading is done when using mobile computing devices. To do so, we use VM. VM is one of the prominent approaches for offloading computational load to cloud server nodes.

A challenging aspect of such frameworks is the additional computing resources utilization in the deployment and management of VM on Smartphone. The deployment of Virtual Machine (VM) requires computing resources for VM creation and configuration. The management of VM includes computing resources utilization in the monitoring of VM in entire lifecycle and physical resources management for VM on Smartphone. (Sanaei 2012)

Chen-Yi Chang et.al (2012)," Power Consumption Optimization for Information Exchange in Wireless-Relay Sensor Networks" has discuss about the power consumption optimization for WSN. Author discuss that the minimization of power consumption is a design goal for wireless relay networks. The wireless communication is optimized to minimize the total transmission power. A wireless relay sensor network is an aggregation of sensor nodes. It has the ability to transmit and receive wirelessly. In this network, the battery powered sensors are used. For this purpose, nodes communicate with each other shall be carefully designed. Communication between nodes requires three actions: transmission, detection, and reception. To reduce the energy consumption in reception mode, a popular approach is to switch the sensor node into sleep mode in which a node shuts off its radio transceiver to disengage itself from the network for a period of time. Compared with the power consumption in transmission mode or reception mode, the power consumption in sleep mode is often negligible. In this paper, we investigate the

optimization of power consumption minimization for information exchange. We further include the detection power and the reception power in order to minimize the overall network power consumption for information exchange in wireless-relay sensor networks.

Mehrdad Ahadi and Amir Masoud Bidgoli (2012)," A Multiple-Sink Model for Decreasing the Energy Hole Problem in Large-Scale Wireless Sensor Networks" has discuss that the communication in the WSN. The data received by the nodes of wireless sensor networks should be sent to the sink. It helps to performing calculations and making the right decisions. The density of data packets increases near the sink. This scenario is known as the Energy Hole. In the WSN the problem of energy hole should be reduced. It is the one of the key factors for designing large scale wireless sensor networks. The multiple sink model is used to reduce the problem of energy hole. It is done by increasing the number of nodes in the vicinity of the sink. This model consists of different levels of sink intensity. The sensor nodes are responsible for processing their surroundings. It sends the collected data to a specific node called sink.

Priyanka et.al (2013),"Cluster Based Efficient Caching Technique for Wireless Sensor Networks" In this paper they establish the method or technique in which Global Cooperative Caching for Sensor Networks is used to improve the Wireless Sensor Network working and consistency. Global Cooperative Caching undertakings association among sensor network's judgement for information objects are depend. Grid based technology is used to improve the battery power and its lifetime. After that this method is added increasing to progress for the network performance. (Sharma 2013)

E Petac,AR Alzoubaidi et.al (2013)," Some Experimental Results About Security Solutions Against DDoS Attacks" The top most security problems in any network is Distributed Denial of Service attack. In modern era the proper solution for it not implemented. The implemented solutions are valid only for limited levels. The detecting and prevent of DDoS attack in Client Server system using informational correlation. This mechanism first store the data into different event regarding with IP packet flow with HS, QHS or AS state. They create PHP module contains the monitoring interface and server. The web monitoring interface collect and display data related to the packets per second rate. If the value exceeding than 50 packets per second (pps) the perl querying interface traffic analyse both real-time and historical information. This IDS only applicable small and medium networks. (Petac 2013)

CHAPTER 3

PROPOSED WORK

3.1 Present Work

In WSN outside and inside attacks are existing, which reduce the ability of the network. In outside attacks a node first of all become the member of the network then harms the whole network whereas the inside attacks the node already in the network known as malicious node and launched attacks on the network.

Security is an important part of any type of network. The achievement of WSN is up to the security how much it is worth for trust. But there are so many numbers of attacks which can target the limitations of the network. For example, the routing is the main and very first step of the network, due to limited recourses the malicious nodes can change the actual path of routing. There are some attacks are possible on some routing protocols (AODV or DSR). The attacks such as Distributed Denial of Service attack, Selective Forwarded attack, Black-hole attack, Sybil attack and Wormhole attack have been identified in various published papers. Currently security is one of the hottest research areas in WSN.

A significant amount of research has been devoted to study security issues as well as countermeasures to various attacks in WSN. However, I believe that there is still much research work needed to be done in the area. The aim of the study is to detect the Distributed Denial of Service attack, Cooperative Black Hole and Sybil attack using AODV protocol in WSN. The Distributed Denial of Service attack is responsible for blocking the service of authorized node or whole the network. The black hole node is responsible for dropping a number from packets after advertising itself as the valid path to source node. In the Sybil attack the single node identify itself as multiple IDs. The detection of these malicious nodes will provide more security to WSN. The Route discovery and route maintenance phases in the AODV protocol will be secured more.

3.2 Objectives

Following are the various objectives of this research work.

- The study focus on analysis of DDoS attacks in WSN.
- The aim of study to detect and prevent the malicious node in the network using AODV routing protocol.
- Analysing the effects of DDoS attacks in the light of working, throughput and network load in WSN.
- To implement new system to detect malicious nodes in the network which are responsible for triggering the attack using a novel schema which is based on Diffie-Hellman and packet received and packet send through it.
- Simulating the detection of DDoS, Black hole, Sybil attack using AODV routing protocol in WSN using MATLAB tool.

3.3 Proposed System

Security in a WSN is a big challenge because of the large number of nodes and self-configure propriety of network. As we know that security is a major issue in WSN because data is continually transmitting through sensor nodes. The attacks which may be possible on Wireless Sensor Network are:

- Distributed Denial of Service (DDoS) Attacks
- Black Hole attack
- Selective Forwarding attack
- Eavesdropping attack
- Wormhole attack
- Sybil attack
- Traffic analysis Attack

So here to prevent some of above attacks we are going to propose a new schema which is based on Diffie-Hellman authentication and some parameter based intrusion detection. These parameters are packet received, packet forward and power.

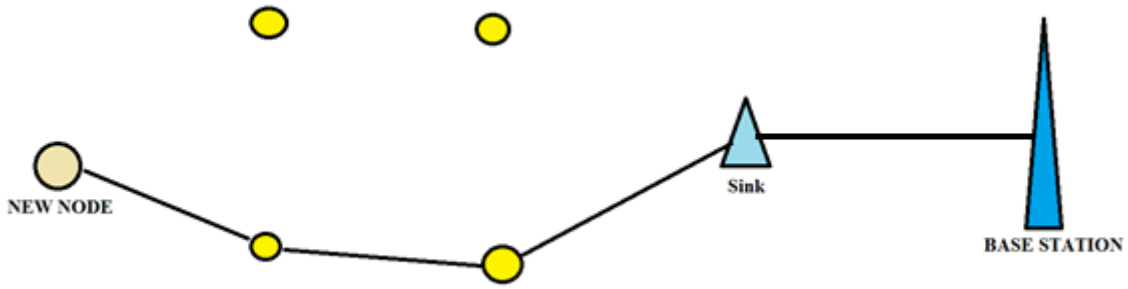

Figure 6: WSN deployment

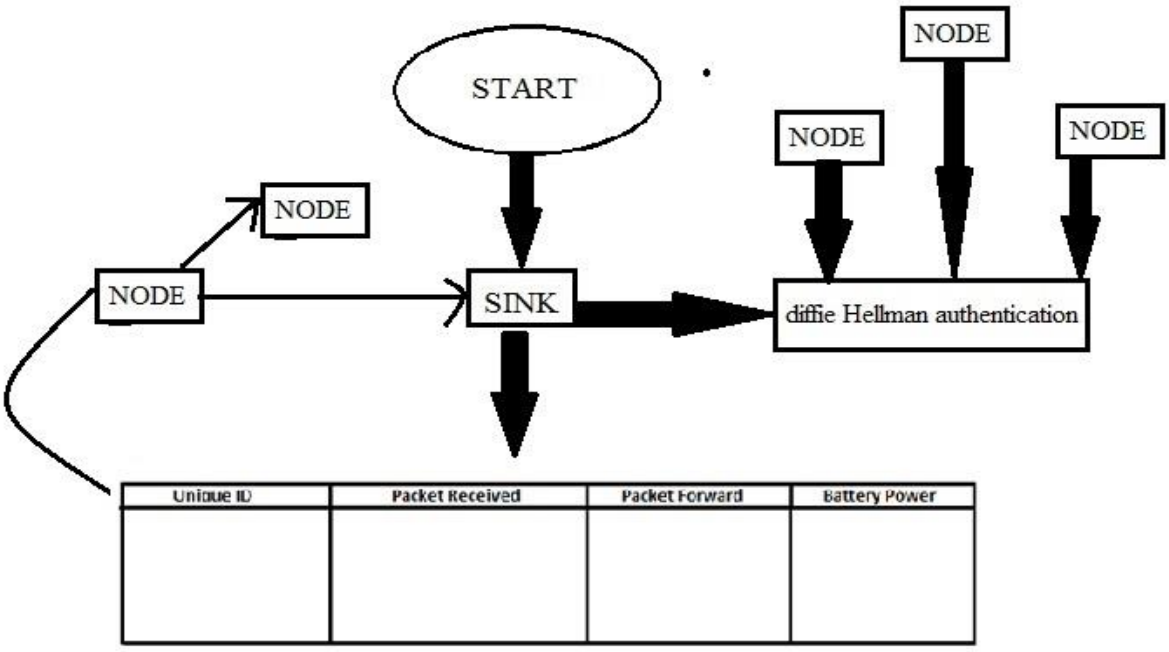

Figure 7: Flow chart

Here sink node will connected to base station. When a new node wants to communicate with the network it will pass through certain steps. New node will be authenticated by the Base station, Base station give a challenge Response Task (CRT) to new node. Now new node will use Diffie-Hellman and give proof of its authentication. Base station will verify

the new node and after verification it will assigned unique ID to it if node will authorized, Therefore it will provide the solution of the Sybil attack.

Now to detect DDoS attack on each node is done through neighbour node. The neighbour node collect packet received and packet forward and battery power or lifetime information and send it to base station after the specific time interval. If the difference between the packets received value and packets forward value will very less thus our network working properly or that node not a malicious node, but the difference between these values is large then the Base station check the last three values of these parameters on same node. If the difference is large as this value BS will understand that this node is malicious node and will isolate or block that malicious node.

But if the value of packet forward will zero from last three time intervals, the BS will understand that the node is Black-Hole node and will isolate or block that malicious node.

Unique ID	Packet Received	Packet Forward	Battery Power

Figure 8: Detection table

Now base station will contain this table for each node and on the bases of this table it will take decision about the node.

Diffie Hellman Algorithm

- Base station and all nodes already known the base g = 5 and prime number value p = 23.
- Base station choose a secret integer a=6 and sends the value of A to node

  $A = g^a \bmod p$

  $A = 5^6 \bmod 23$

  $A = 15{,}625 \bmod 23$

  $A = 8$

- Node choose a secret integer b = 15, then sends the value of B to Base station

  $B = g^b \bmod p$

  $B = 5^{15} \bmod 23$

  $B = 30{,}517{,}578{,}125 \bmod 23$

  $B = 19$

- Base station computes the $s = B^a \bmod p$

  $s = 19^6 \bmod 23$

  $s = 47{,}045{,}881 \bmod 23$

  $s = 2$

- Node computes the $s = A^b \bmod p$

  $s = 8^{15} \bmod 23$

  $s = 35{,}184{,}372{,}088{,}832 \bmod 23$

  $s = 2$

CHAPTER 4

RESULT AND DISCUSSIONS

WSN security is one of the major concerns because of the lack of regular changing topologies. One of the major task is to design a security effective protocol that will help to avoid the attacks and provide a secure communication between the nodes. In a group communication security issues become worst because there are number of senders and number of receivers. So I am going to propose a new system that will be more efficient against the Black and DDOS attacks and helps to detect and prevent the attacks. The proposed work will also enhance the performance of the network.

4.1 SIMULATION

Initial GUI contain different controls on different button.

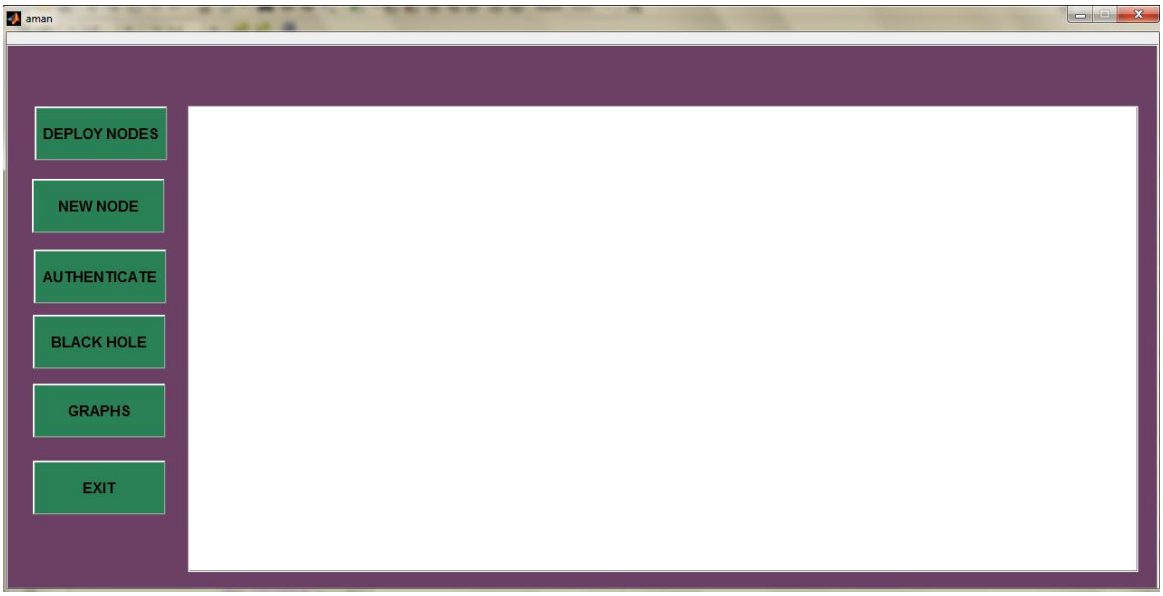

Figure 9: Simulation interface

Deploy number of nodes on random position. Also contain the sink node and base station.

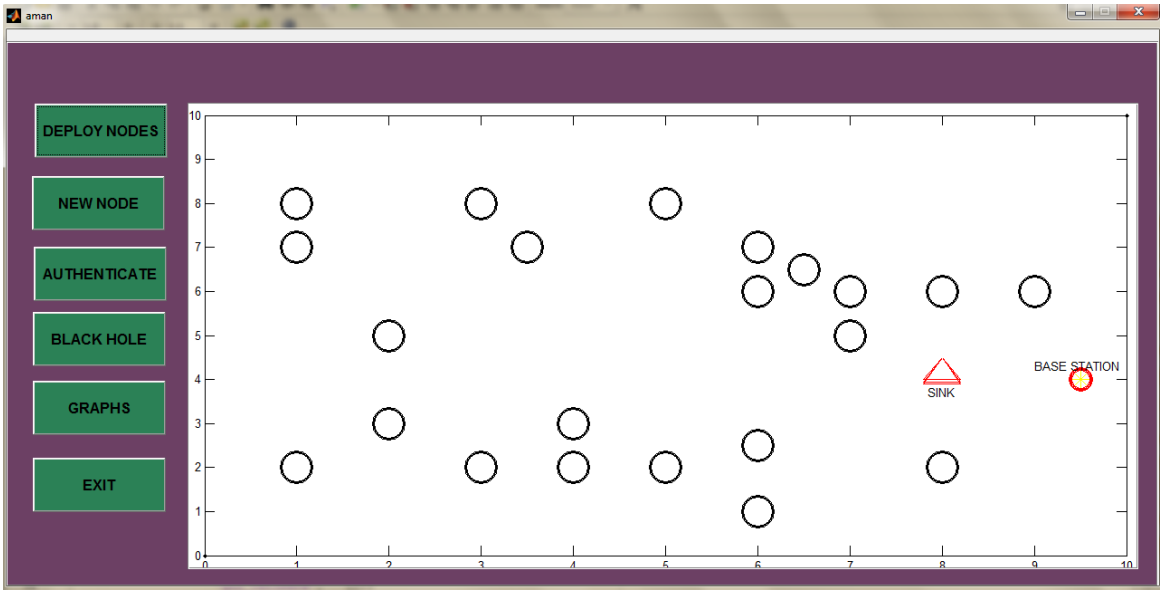

Figure 10: WSN nodes deployment

A new node enter in the network.

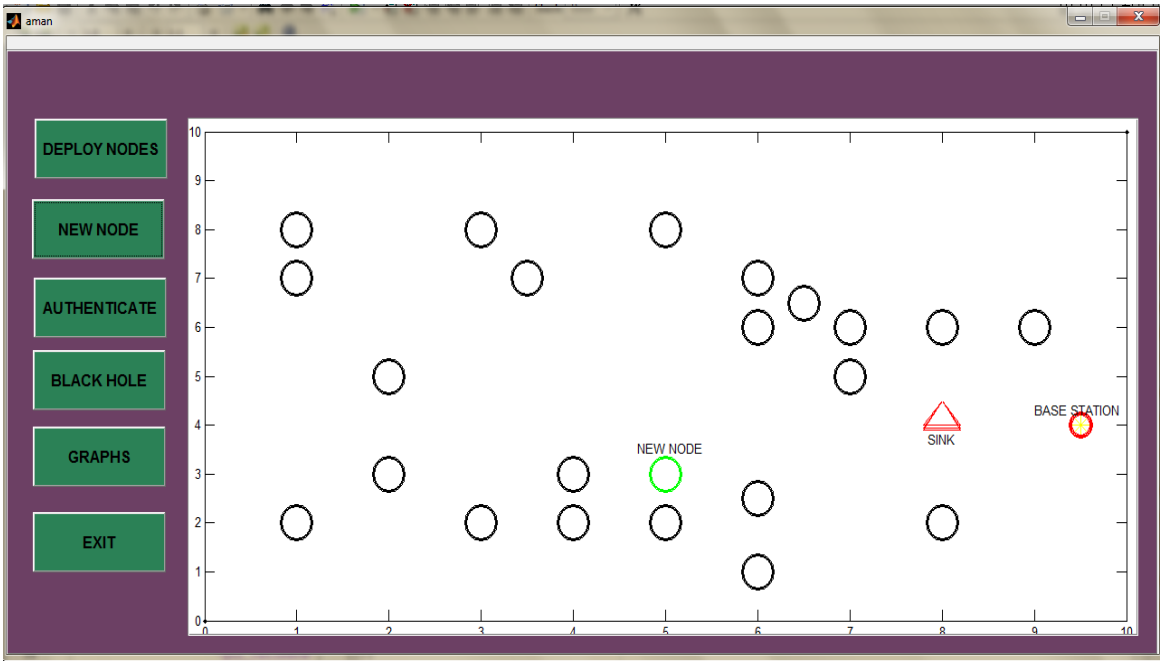

Figure 11: New node

Authentication of the new node is done through the Deffie-Hellman algorithm. New node will choose the two predefined prime values and share those values with the sink node.

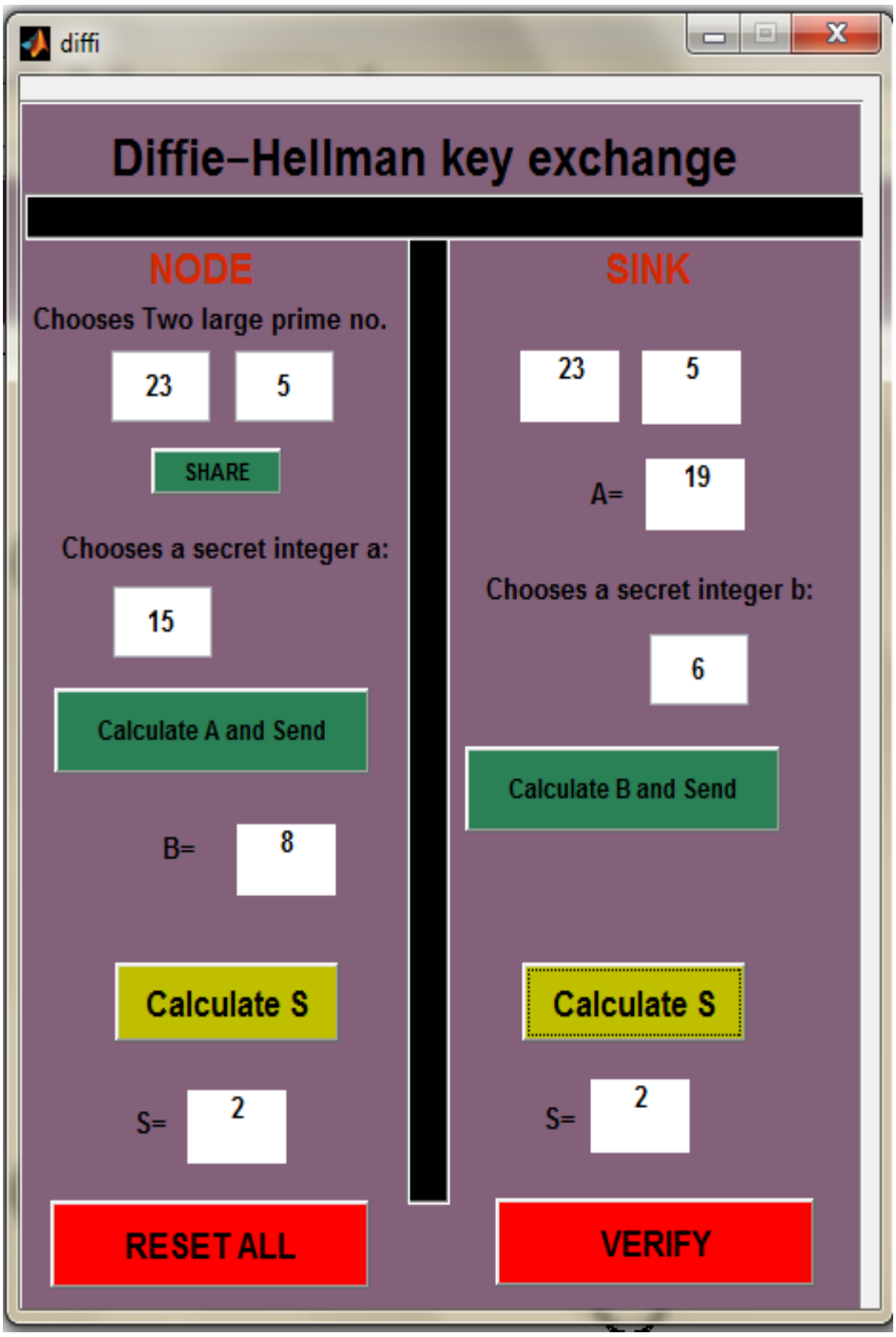

Figure 12: Authentication of new node

New node will choose a secret key named as ‘a’ and calculate the value of ‘A’ and share it with the sink node. Now the sink node will choose a secret key named as ‘b’ and calculate the value of ‘B’ and share it with the new node. After that both nodes will calculate the value of ‘S’.

If the value of ‘S’ matches then new node is a valid node otherwise it is an invalid node.

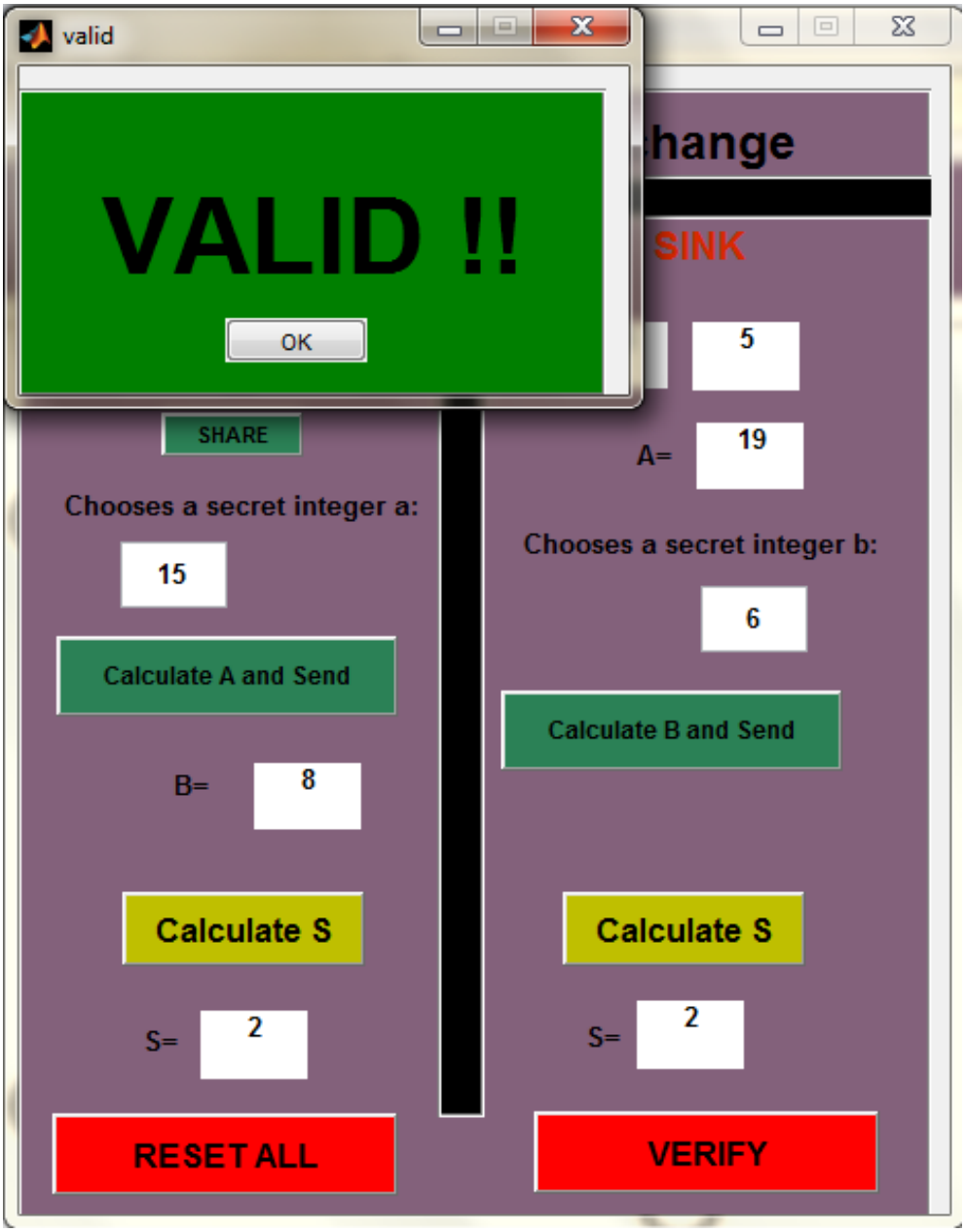

Figure 13: Valid node

After validation new node will send the information to sink node for further communication.

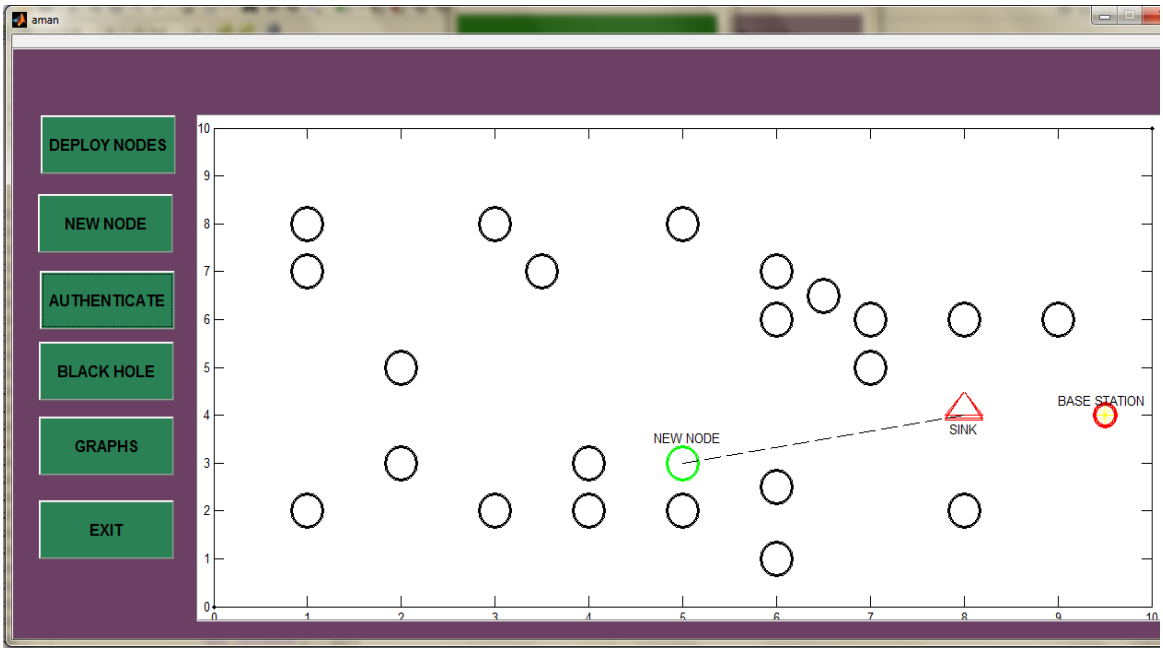

Figure 14: Node communication

New node will start communication with the other sensor nodes existing in the network.

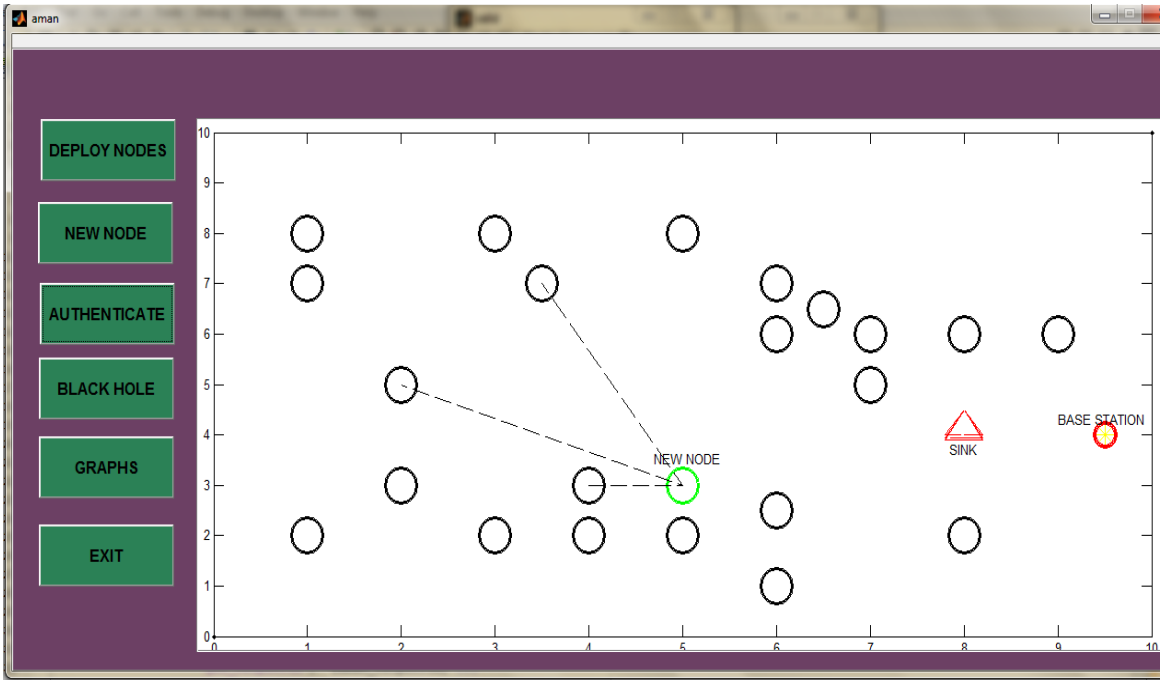

Figure 15: Node communication

Now the neighbor of new node will collect its past data transition history and send to the sink node.

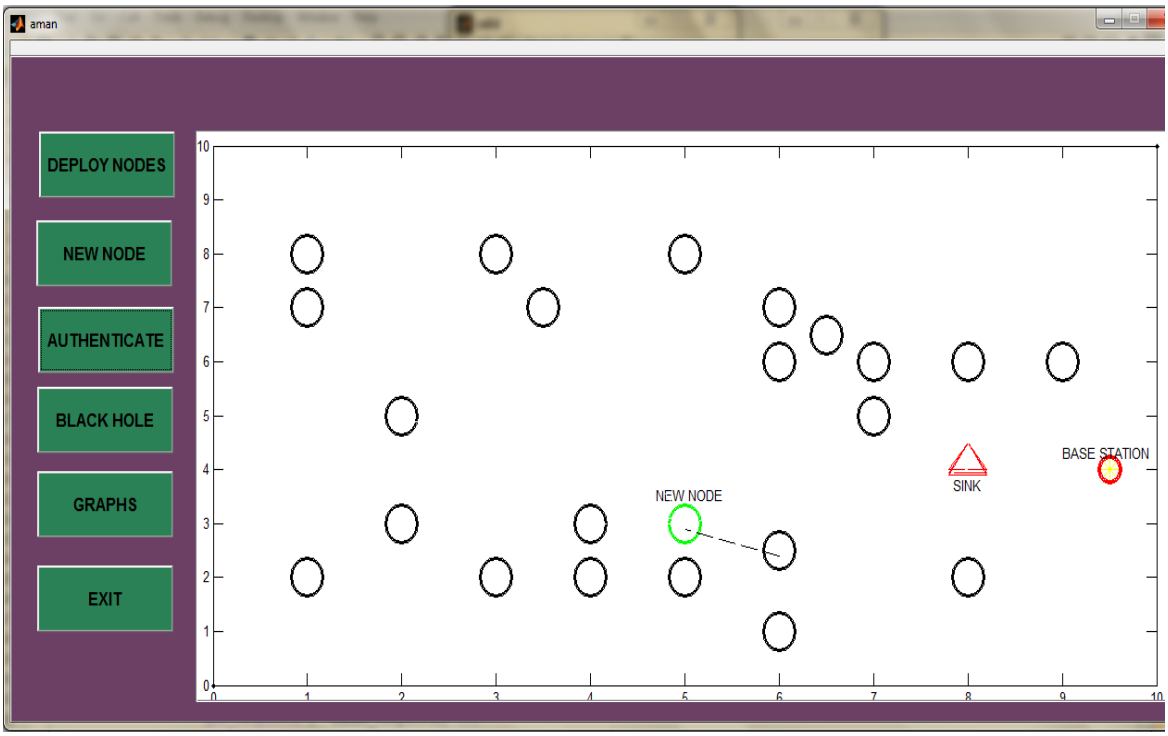

Figure 16: Detection of new node

The data transition history contains packet received, packet forward, battery power and unique ID of the new node.

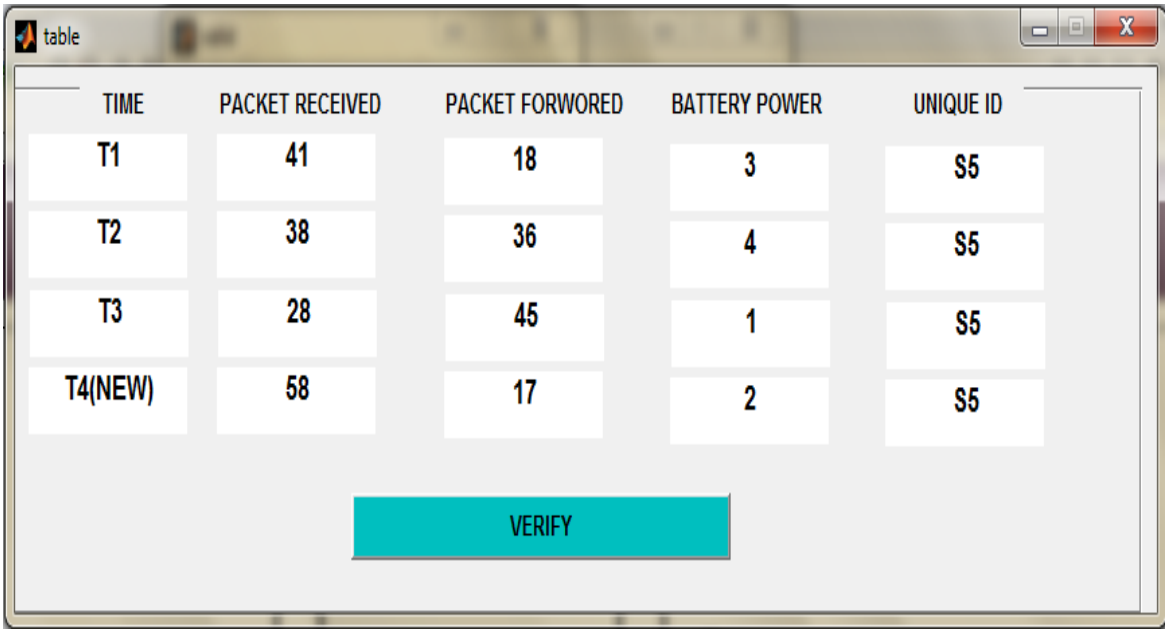

Figure 17: Data transition history

If the data transition history is appropriate than this node will be assigned as valid node otherwise it is declared as malicious node.

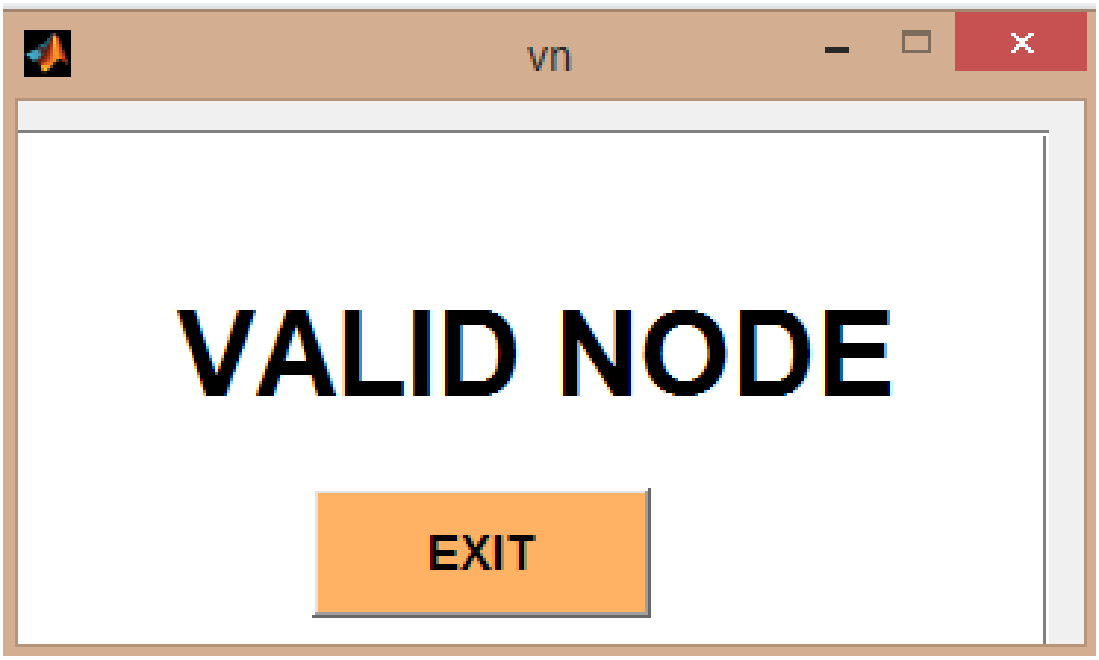

Figure 18: Valid node

If the data transition history is appropriate than this node will be assigned as valid node otherwise it is declared as malicious node.

Figure 19: Invalid node

Black hole malicious node dropping all the data packets received instead of forwarding to the next neighbor node present in the network. The detection of the black hole node will be completed through the available data transition history of the node. If node receiving all the data packets and not forwarding a single packet to the next neighbor node will be declared as black hole malicious node and isolated from the network.

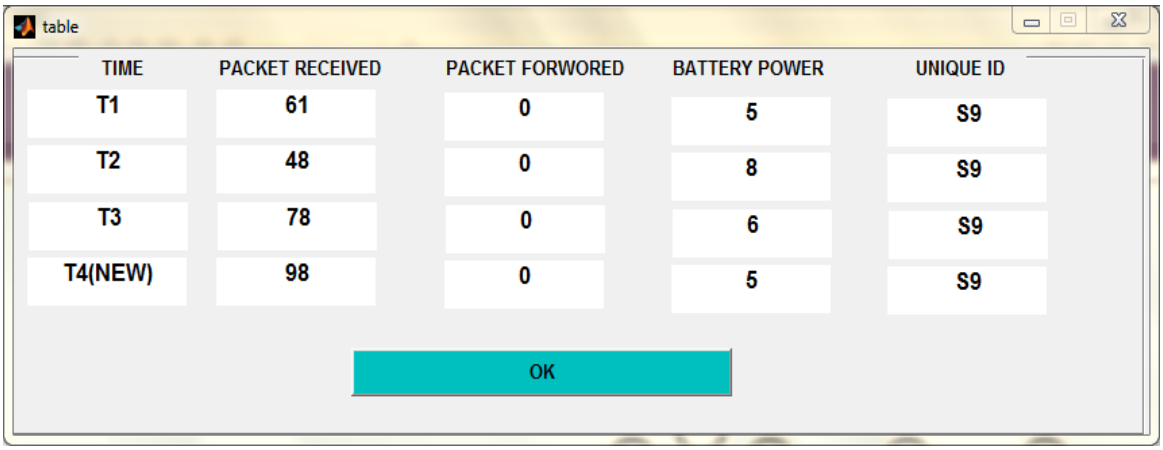

Figure 20: Data transaction history

The below figure shows the black hole node dropping all the data instead of forwarding it to the next neighbor node.

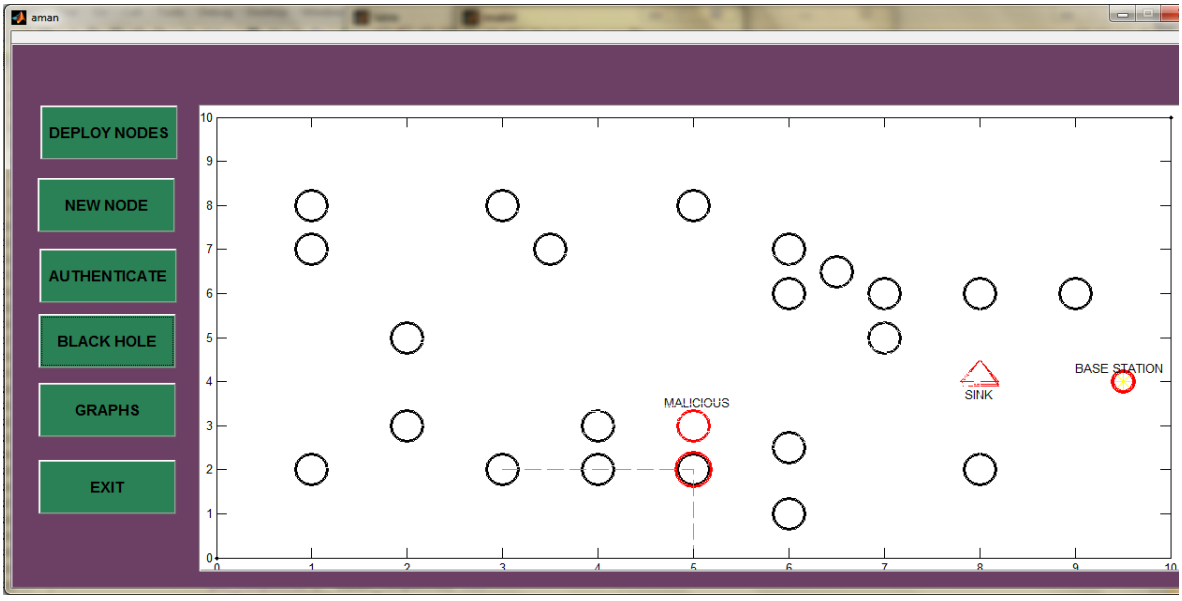

Figure 21: Black hole node

Sink node will send the message to all the available sensor nodes about the present of malicious nodes in the network and told them to stop the communication with the maliciuos nodes.

This proposed solution will improve the security of wireless sensor network and make it more reliable.

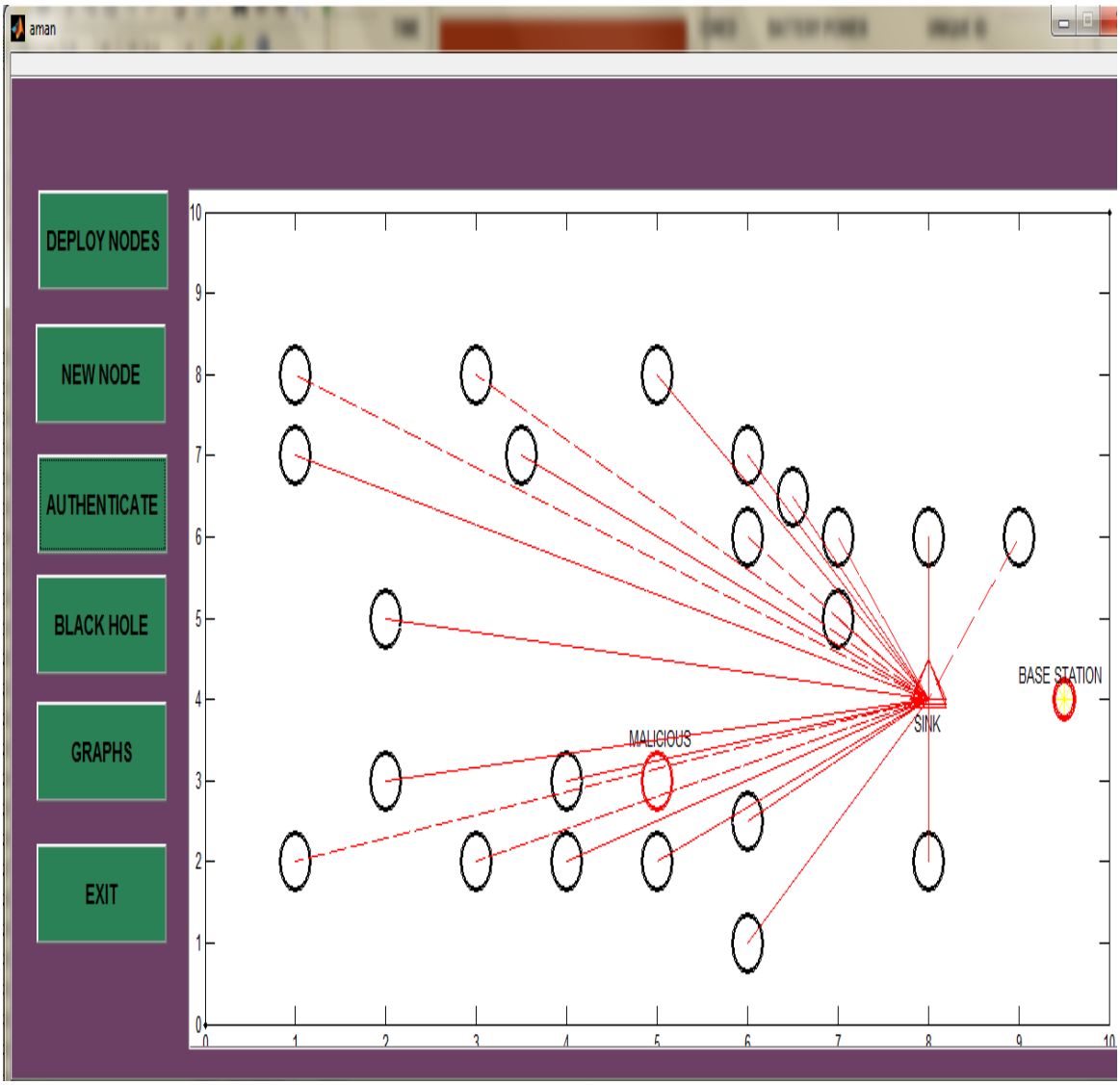

Figure 22: Malicious node message

4.2 PERFORMANCE COMPARISION

4.2.1 Throughput graph

The following graph shows the comparison between the old work and new work in form of throughput. The new work shows the enhancement in the network in form of throughput.

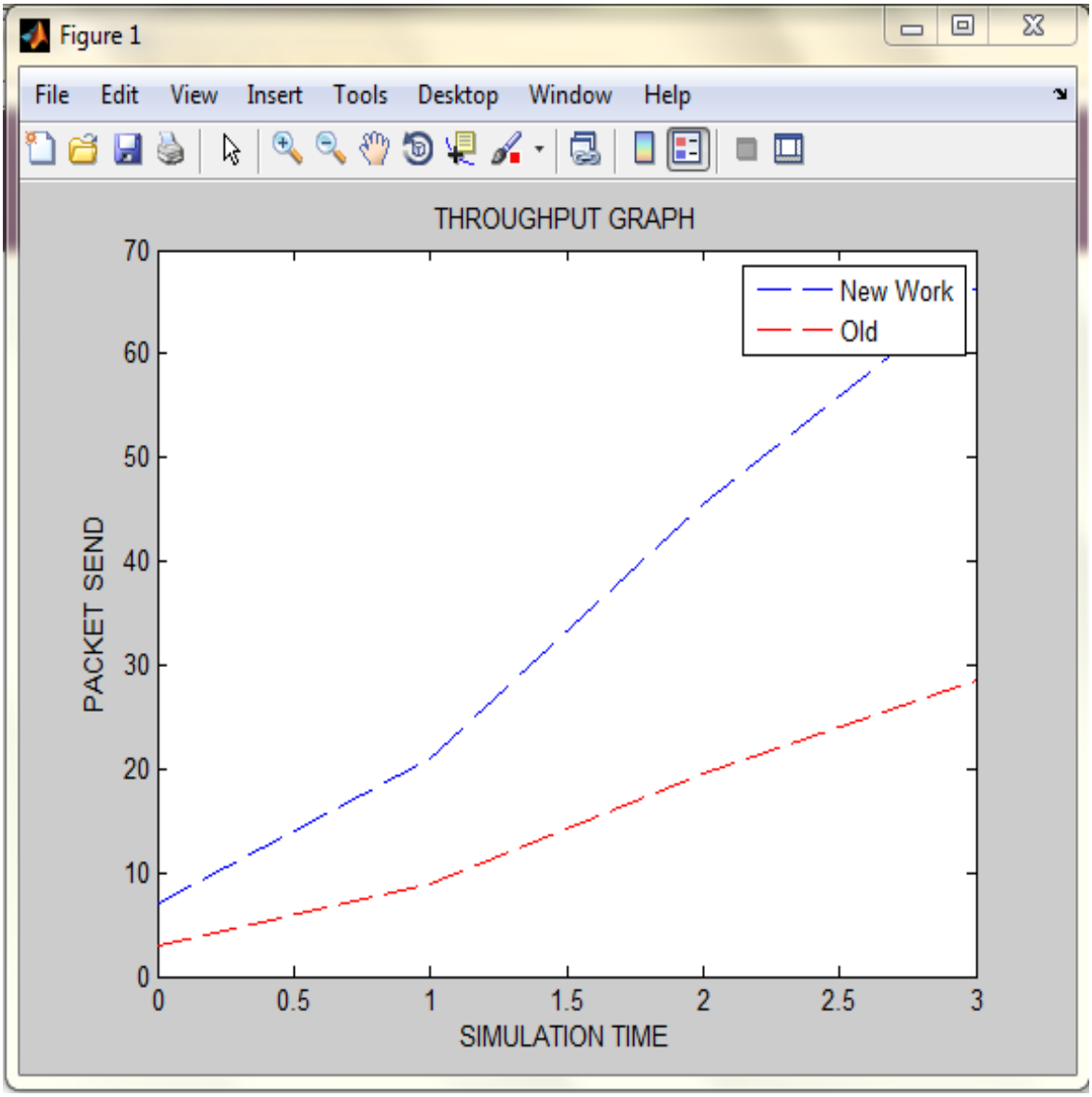

Figure 23: Throughput graph

4.2.2 Delay graph

The following graph shows the comparison between the old work and new work in form of delay. The new work shows the decrease in delay in the network.

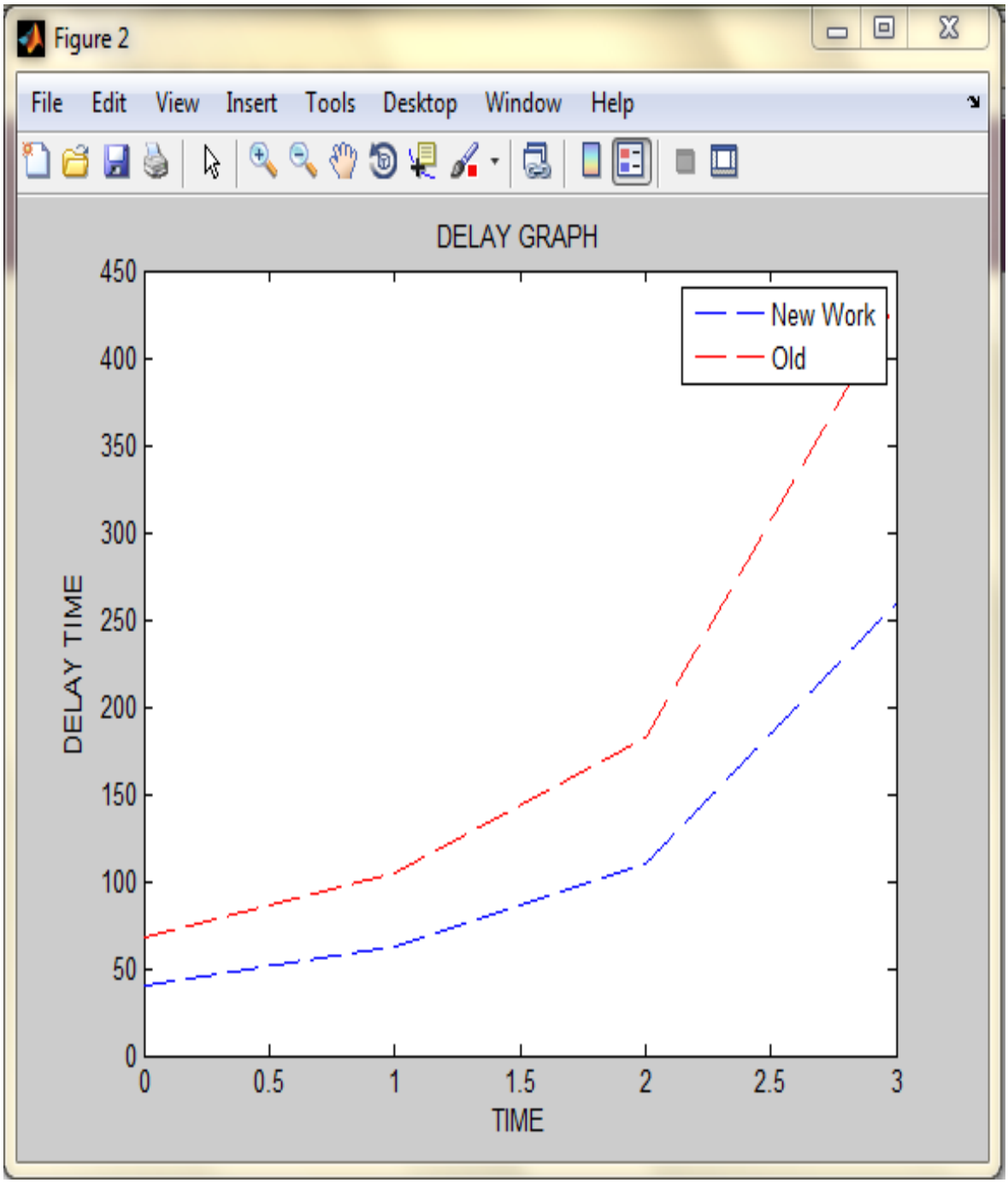

Figure 24: Delay graph

4.2.3 Congestion graph

The following graph shows the comparison between the old work and new work in form of congestion. The new work shows the decrease in congestion of the network.

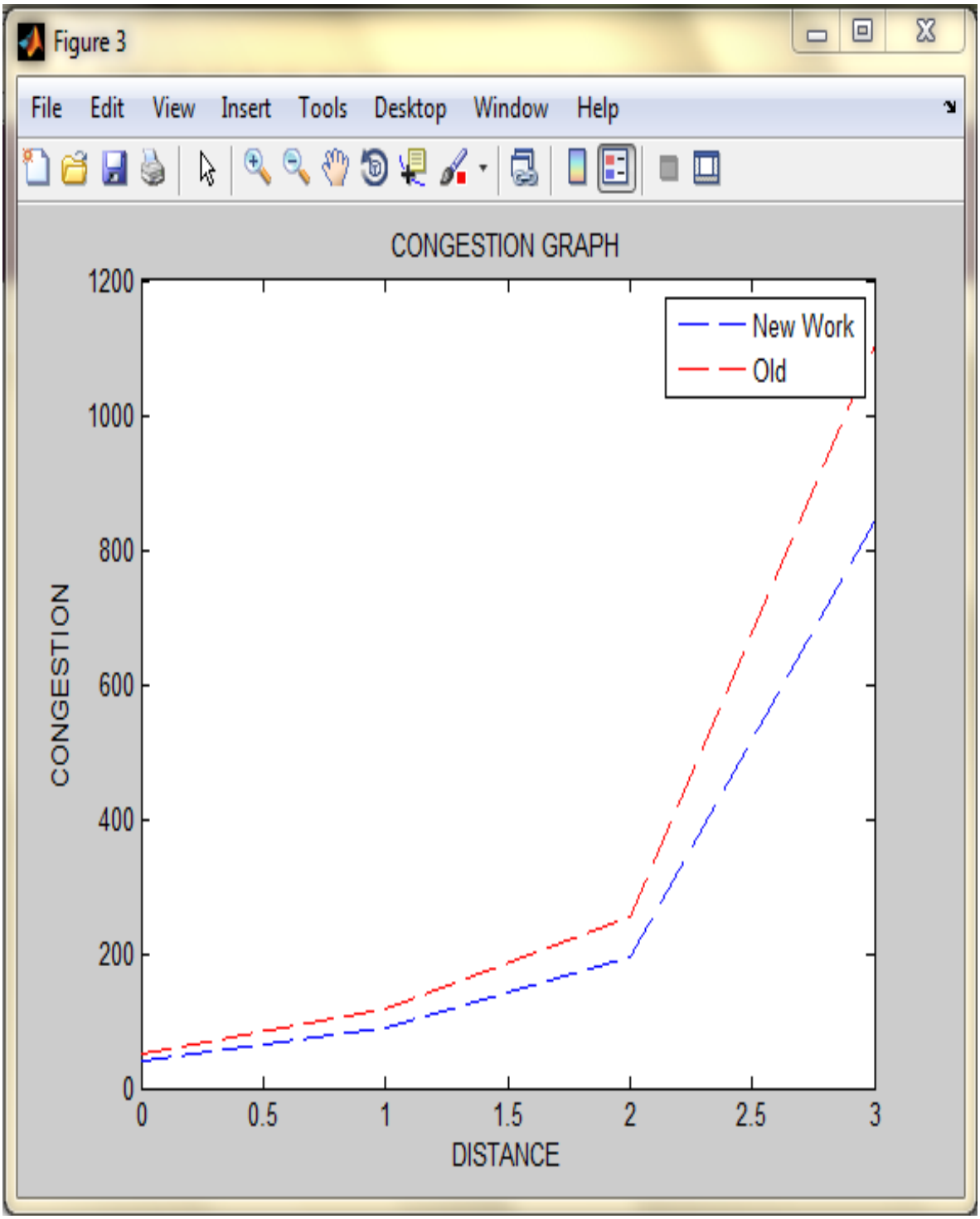

Figure 25: Congestion graph

4.2.3 PDR graph

The following graph shows the comparison between the old work and new work in form of Packet Delivery Ratio (PDR). The new work shows the enhancement in Packet Delivery Ratio of the network.

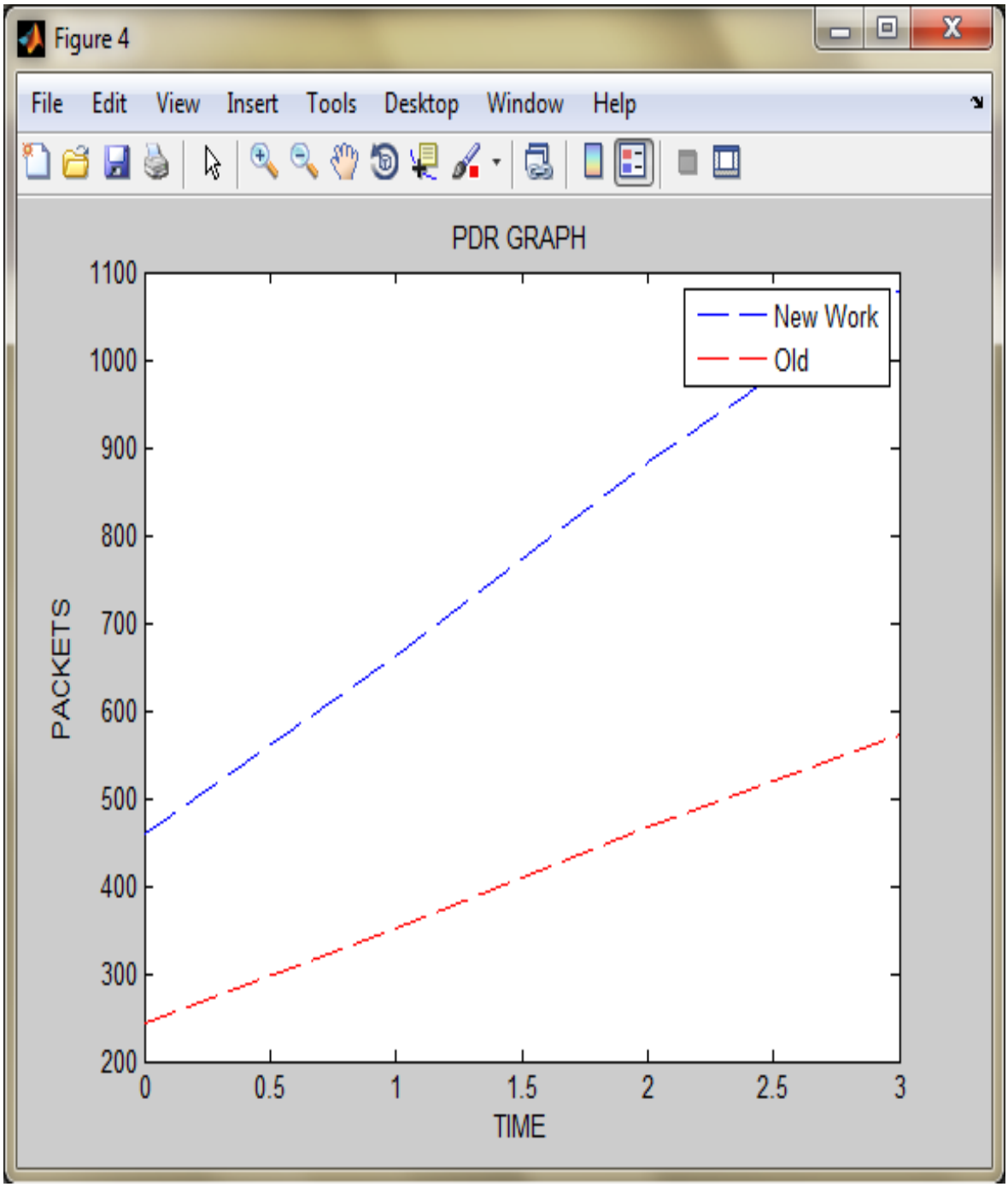

Figure 26: PDR graph

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

This proposed work is about the Wireless Sensor Network and security of it. The output of this work will be the detection and prevention of major attacks like Distributed Denial of Service, Black-Hole attack and Sybil attack. In this work we proposed a secure mechanism with based on some authentication steps related to Diffie-Hellman algorithm then mechanism will detecting and preventing Distributed denial of service, Black Hole, Sybil attacks using some network parameters mainly packet received, packet forwarded and battery power. Distributed Denial of Service attack forwarded large number of packets on the network and interrupt the legitimate nodes, whereas Black-Hole node dropped all the valuable packets and Sybil attack identity itself more than once at a time, So using this mechanism malicious node will detected and isolated or blocked for further communication on the network. A sensor network consisting from sensor node which deployed on the unreachable places. Every node made up with the sensing system, very less computational power and limited battery lifetime with many security problems. Sensor nodes sense the environment, process the data obtained by the node and forward this data to Base Station located some far from the sensor network through sink node. The study shows a secure mechanism which is based on some authentication steps related to Diffi-Hellman algorithm. Our mechanism is detecting and preventing Distributed denial of service, Black Hole, Sybil attacks and make wireless sensor network more reliable and secure for communication.

The future work of the study is to enhance the proposed technique to detect more such types of attacks like Gray hole attack and make wireless sensor network for secure for communication. The further implementation will include more WSN nodes and prevent the above discuss attacks

REFERENCES

I. RESEARCH PAPERS

[1] Ahamed, SS Riaz. "The role of zigbee technology in future data communication system." *Journal of theoretical and applied information technology*, 2009: 129-135.

[2] Akyildiz, Ian F., Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. "Wireless sensor networks: a survey." *Computer networks 38, no. 4*, 2002: 393-422.

[3] Ali, Muneeb, Umar Saif, Adam Dunkels, Thiemo Voigt, Kay Römer, Koen Langendoen, Joseph Polastre, and Zartash Afzal Uzmi. "Medium access control issues in sensor networks." *ACM SIGCOMM Computer Communication Review 36, no. 2* , 2006: 33-36.

[4] Chauhan, Naveen, L. K. Awasthi, and Narottam Chand. "Global cooperative caching for Wireless Sensor Networks." *In Information and Communication Technologies (WICT), IEEE*, 2011: 235-239.

[5] Diamond, Scott M., and Marion G. Ceruti. "Application of wireless sensor network to military information integration." *In Industrial Informatics, 2007 5th IEEE International Conference*, 2007: vol. 1, pp. 317-322.

[6] Kant, Kamal, and Nitin Gupta. "Application based Study on Wireless Sensor Network." *International Journal of Computer Applications*, 2011.

[7] Karlof, Chris, and David Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures." *Ad hoc networks 1, no. 2* , 2003: 293-315.

[8] Kaur, Parminder, and Ravikant Sahu. " TO ENHANCE THE LIFETIME OF WIRELESS SENSOR NETWORK USING A NOVEL APPROACH BASED ON NEURAL NETWORK." *ijcsme.com*, 2014.

[9] Li, Xu, Amiya Nayak, and Ivan Stojmenovic. "Sink mobility in wireless sensor networks." *Wireless Sensor and Actuator Networks*, 2010: 153.

[10] Okdem, Selcuk, and Dervis Karaboga. "Routing in wireless sensor networks using an ant colony optimization (ACO) router chip." *mdpi.com*, 2009: Sensors 9, no. 2 (2009): 909-921.

[11] Pathania, Shruti, and Parminder Singh. "Energy Efficient Mechanism to Enhance the Life Time of Wireless Sensor Network." *ijaret.org*, n.d.

[12] Petac, Eugen, Abdel Rahman Alzoubaidi, and Petrut Duma. "Some experimental results about security solutions against DDoS attacks." *In Signals, Circuits and Systems (ISSCS), 2013 International Symposium on, pp. 1-4. IEEE*, 2013.

[13] Sanaei, Zohreh, Saeid Abolfazli, Abdullah Gani, and Muhammad Shiraz. "SAMI: Service-based arbitrated multi-tier infrastructure for mobile cloud computing." *In Communications in China Workshops (ICCC), 2012 1st IEEE International Conference* , 2012: 14-19.

[14] Sharma, Priyanka, and M. K. Rai. "Review paper on Cluster Based Caching Technique for Wireless Sensor Networks with multi-sink." *International Journal for Advance Research in Engineering and Technology 1, no. 2*, 2013.

[15] Shiri, Amir, Shahram Babaie, and Javad Hasan-zadeh. "New Active Caching Method to Guarantee Desired Communication Reliability in Wireless Sensor Networks." *Journal of Basic and Applied Scientific Research*, 2012.

[16] Sohraby, Kazem, Daniel Minoli, and Taieb Znati. "Wireless sensor networks: technology, protocols, and applications. ." *John Wiley & Sons*, 2007.

II. Books

[1] argie, Waltenegus, and Christian Poellabauer. *Fundamentals of wireless sensor networks: theory and practice.* . John Wiley & Sons, 2010.

[2] Walters, John Paul, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary. "Security in distributed, grid, mobile, and pervasive computing 1." In *Wireless sensor network security: A survey.*, by John Paul, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary. Walters, 367. 2007.